

Міністерство освіти і науки України
Національний університет «Запорізька політехніка»

Методичні вказівки
до виконання лабораторних робіт з дисципліни

МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

для студентів спеціальності
172 «Електронні комунікації та радіотехніка»,
які навчаються за освітньою програмою «Радіотехніка»
всіх форм навчання
(частина 2)

2024

Методичні вказівки до виконання лабораторних робіт з дисципліни “Методи і засоби захисту інформації” для студентів спеціальності 172 «Електронні комунікації та радіотехніка», які навчаються за освітньою програмою «Радіотехніка» всіх форм навчання. Частина 2 / Укл. Сметанін І.М. – Запоріжжя: НУ «Запорізька політехніка», 2024. – 66 с.

Укладач: Сметанін І.М., старший викладач

Рецензент: Костенко В.О., доцент, канд .техн. наук.

Відповідальний за випуск: Сметанін І.М., старший викладач

Затверджено
на засіданні кафедри радіотехніки та
телекомунікацій.
Протокол № 4 від 15 лютого 2024 р.

Затверджено
на засіданні НМК факультету
ФІБЕК
Протокол №5 від 15 лютого 2024 р.

ЗМІСТ

ЗМІСТ	3
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ	5
ВСТУП	6
4. ЛАБОРАТОРНА РОБОТА №4. ВИВЧЕННЯ	
ХАРАКТЕРИСТИК ТА БУДОВИ ПРИСТРОЮ СРМ-700	
(«АКУЛА»).....	7
4.1 Мета роботи	7
4.2 Загальні відомості	7
4.2.1 Методи та прилади виявлення фактів підслуховування у	
телефонних лініях	8
4.2.2 Можливості приладу СРМ-700 «АКУЛА» у виявленні	
пристроїв прослуховування телефонних і інших ліній.....	11
4.3 Завдання на підготовку до лабораторної роботи.....	13
4.4 Контрольні запитання для самоперевірки і контролю	
підготовленості студентів до роботи.....	14
4.5 Матеріали, інструмент, прилади, обладнання	14
4.6 Вказівки з техніки безпеки	15
4.7 Порядок проведення лабораторної роботи	16
4.7.1 Виявлення радіопередавачів.....	16
4.7.2 Порядок перевірки телефонних апаратів і телефонної лінії	21
4.7.3 Перевірка розподільчих коробок та телефонних кросів.....	24
4.7.4 Фізичний пошук	25
4.7.5 Перевірка ліній електроживлення	25
4.7.6 Перевірка лінійного господарства	27
4.8 Зміст звіту	28
4.9 Рекомендована література	28
5. ЛАБОРАТОРНА РОБОТА №5. ДОСЛІДЖЕННЯ	
ГЕНЕРАТОРУ АКУСТИЧНОГО ЗАШУМЛЕННЯ ANG-2200	29
5.1 Мета роботи	29
5.2 Загальні відомості	29
5.2.1 Призначення генератору ANG-2200	29
5.2.2 Принцип дії та технічні характеристики генератору ANG-2200	
.....	30
5.2.3 Робота з генератором.....	33
5.3 Завдання на підготовку до лабораторної роботи.....	40
5.4 Контрольні запитання для самоперевірки і контролю	
підготовленості студентів до роботи.....	40

5.5 Матеріали, інструмент, прилади, обладнання	42
5.6 Вказівки з техніки безпеки	43
5.7 Порядок проведення лабораторної роботи	44
5.8 Зміст звіту	45
5.9 Рекомендована література	45
6 ЛАБОРАТОРНА РОБОТА №6. ДОСЛІДЖЕННЯ	
МАСКУВАЧА МОВНИХ СИГНАЛІВ	46
6.1 Мета роботи	46
6.2 Загальні відомості	46
6.2.1 Скремблери.....	46
6.2.2 Аналогове скремблювання	49
6.2.3 Цифрове скремблювання	56
6.2.4 Критерії оцінки систем приховування мови	60
6.3 Завдання на підготовку до лабораторної роботи.....	62
6.4 Контрольні запитання для самоперевірки і контролю підготовленості студентів до роботи.....	62
6.5 Матеріали, інструмент, прилади, обладнання	63
6.6 Вказівки з техніки безпеки	63
6.7 Порядок проведення лабораторної роботи	64
6.8 Зміст звіту	65
6.9 Рекомендована література	65
6.10 Додатки	66
Додаток 6.А.....	66

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

FM – frequency modulation (частотна модуляція)

AM – амплітудна модуляція

АРУ – автоматичне регулювання підсилення

НВЧ – надвисокі частоти

РРЛ – радіорелейна лінія

СКД – служба космічних досліджень

СКЕ – служба космічної експлуатації

ВСТУП

Стан захищеності інформації забезпечується як рівнем захищеності безпосередньо інформації, так і її носіїв (людей, стану інформаційних систем, систем охорони і захисту) від різного виду загроз. Джерела таких загроз можуть бути навмисними, які ставлять за мету несанкціоноване отримання інформації, і ненавмисними, що такі цілі не переслідують.

Технічні канали витоку інформації зумовлено різноманітними процесами і явищами, які відбуваються під час функціонування майже всіх електричних і електронних пристроїв. Фізичні процеси, що мають місце під час роботи різноманітних пристроїв, лежать в основі появи каналів несанкціонованого доступу до інформації, що обробляється або передається такими пристроями. Тому спеціалісти з питань захисту інформації, у свою чергу, шукають такі методи, засоби та рішення, які забезпечують процес захисту інформації.

Цикл лабораторних робіт з дисципліни «Методи і засоби захисту інформації» доповнює об'єм практичних і теоретичних знань, які отримує студент під час вивчення цього навчального курсу.

Методичні вказівки до лабораторних робіт складені з двох частин. В першу частину увійшли лабораторні роботи, які сприяють повнішому засвоєнню матеріалу про загальні принципи організації захисту інформації в радіотехнічних і телекомунікаційних системах і мережах на базі сучасних концепцій, а також принципів побудови і функціонування професійних облаштувань несанкціонованого знімання інформації в радіотехнічних і телекомунікаційних системах і мережах. Друга частина лабораторних робіт сприяє повнішому засвоєнню матеріалу по способах технічного виявлення джерел витоку інформації і методам захисту інформації в радіотехнічних, телекомунікаційних та інформаційних системах.

4. ЛАБОРАТОРНА РОБОТА №4. ВИВЧЕННЯ ХАРАКТЕРИСТИК ТА БУДОВИ ПРИСТРОЮ СРМ-700 («АКУЛА»)

4.1 Мета роботи

Метою лабораторної роботи є перевірка властивостей та здатності пристрою СРМ-700 («АКУЛА») виявляти наявність прослуховуючих пристроїв, які встановлені на акустичний канал витоку розмовної інформації.

4.2 Загальні відомості

Актуальність захисту телефонних переговорів поставила перед користувачами засобів спеціальної техніки завдання розпізнавання і пошуку пристроїв знімання інформації для їх наступної нейтралізації. У цей час ринок виробів спеціальної техніки представлений широким вибором приладів, що дозволяють із тим або іншим ступенем вірогідності виявляти наявність прослуховуючих пристроїв, встановлених на телефонній лінії.

Перевірка підключення, присутності радіомікрофонів або систем "нав'язування" у телефонних лініях і апаратах звичайно здійснюється шляхом вимірювань рівня сигналу в лінії у робочому положенні, тобто при піднятій трубці телефону. Наявність жучка визначається прослуховуванням набору номера через навушники. Під час таких вимірювань необхідно використовувати джерело "відомого звуку".

Взагалі, тривалі записи, наприклад, бізнес-звіти або огляди сільськогосподарського ринку, можна використовувати як джерело "відомого звуку" для маскування ваших дій.

За принципом дії прилади виявлення пристроїв, що підслуховують, можна умовно розділити на наступні групи:

- Прилади контролю напруги лінії;
- Прилади контролю навколишнього радіоефіру;
- Прилади контролю сигналів у телефонній лінії;
- Прилади аналізу неоднорідності телефонної лінії;
- Прилади аналізу не симетрії лінії;
- Прилади аналізу не лінійності параметрів лінії.

4.2.1 Методи та прилади виявлення фактів підслуховування у телефонних лініях

Прилади контролю напруги лінії утворюють найбільш численну групу приладів виявлення підключень до лінії. Прилади даної групи реєструють зміни напруги лінії за допомогою компараторів або вольтметрів. При цьому якщо напруга на лінії змінюється на достатню величину, то робиться висновок про гальванічне підключення до лінії. Основним недоліком всіх приладів даної групи є те, що вони повинні бути встановлені на "чисту" лінію, тобто виявляються тільки нові гальванічні підключення до лінії. Наприклад, всі прилади даної групи успішно виявляють «підняття» трубки паралельного телефону в момент проведення переговорів по лінії або підключення до лінії "нових" телефонних закладок з живленням від лінії (послідовних з опором більше 0,5 кОм, паралельних з опором менш 10 кОм). При вимірюванні напруги лінії за допомогою вольтметрів або компараторів варто враховувати "природні" коливання напруги лінії в межах до 1В, залежність параметрів лінії від температури, вологості, стану устаткування АТС, опору перехідних колодок і інших факторів

Прилади контролю навколишнього радіоефіру дозволяють проводити пошук активних радіомікрофонів (радіозакладок) у приміщенні, обстежити телефонну лінію, електромережу та інші лінії зв'язку для виявлення працюючих закладок з радіоканалом, побічних випромінювань, радіопроменю і багато іншого. До даного типу пристроїв відносяться скануючі приймачі, індикатори поля, спеціальні частотоміри і аналізатори спектра, спектральні корелятори, комплекси радіоконтролю і т.і. Основними перевагами цієї групи приладів є вірогідність отриманої інформації про наявність пристроїв, що прослуховують, з радіоканалом, можливість відшукування радіопередавального пристрою. До недоліків способу можна віднести малу відстань виявлення "жучків", обов'язкову активізацію пристроїв, що прослуховують, при їхньому пошуку, значний час контролю ефіру, що утрудняє оперативний контроль телефонної лінії.

Принцип дії **приладів контролю сигналів на телефонній лінії** заснований на частотному аналізі сигналів, наявних на провідній лінії (електромережа, телефонна лини, кабельні лінії сигналізації і т.і.). Як правило, прилади цієї групи працюють у діапазоні частот 40 Гц ...10 МГц, мають високу чутливість (на рівні 20 мкВ), розрізняють модуляцію

прийнятого сигналу, мають можливість контролю прийнятої інформації. За допомогою даних приладів можна легко встановити факт передачі інформації з лінії, "ВЧ-нав'язування" і ін.

Контроль сигналів на телефонній лінії часто виконують більше складні багатофункціональні прилади (наприклад, OSCOR-5000, CPM-700 і ін.).

Прилади аналізу неоднорідності телефонної лінії визначають зосереджені резистивні або реактивні провідності, що підключені до лінії. Здійснюється це шляхом вимірювання параметрів сигналу (найчастіше потужності), відбитого від неоднорідності лінії. Зразки приладів, цього класу (наприклад, БОР-1), що періодично з'являються на ринку, дозволяють визначити відстань до неоднорідності. Однак невелика дальність виявлення (реально до 500 м), низька вірогідність отриманих результатів вимірів роблять прилади цієї групи ефективними тільки для реєстрації «нових» підключень до лінії при невеликих вимірюваних відстанях, оскільки найчастіше за неоднорідність приймаються контактні з'єднання в лінії. Висока ціна й складність реалізації даного способу виявлення, перешкоджають практичному поширенню приладів.

Найпоширенішим із **приладів аналізу не симетрії лінії** є ТПУ-5. Принцип дії приладу заснований на визначенні різниці опорів проводів лінії на змінному струмі й визначенні втрат по постійному струму між проводами лінії. Вимірювання проводяться щодо нульового проводу електромережі. Прилад не вимагає "чистої" лінії при роботі. Чутливість його досить висока для виявлення практично будь-яких закладок, контактної підключення до лінії. Прилад виявляє послідовно включені пристрої прослуховування, із внутрішнім опором більшим за 100 Ом і паралельні - зі струмом споживання більше 0,5 мА. Прилад має й ряд недоліків. У разі початкової не симетрії лінії (наприклад, за рахунок старої і розгалуженої проводки усередині будинку, наявності скруток, відводів, контактних з'єднань і т.п.) прилади даної групи помилково вказують на наявність послідовно підключеного підслуховуючого пристрою. Використання в якості "третього" проводу нульової шини електромережі у випадку несправності в приладі може привести до виходу з ладу устаткування АТС, телефонної лінії.

В останні кілька років з'явилися **прилади аналізу не лінійності параметрів лінії**, принцип дії яких заснований на аналізі не лінійності імпедансу телефонної лінії. У свою чергу в цій групі приладів існують

дві підгрупи. Це прилади, що визначають не лінійність двопроводної знеструмленої лінії і прилади, що працюють на реальній телефонній лінії. Прилади, що визначають не лінійність двопроводної знеструмленої лінії (АТ-2, ВІЗІР і ін.) мають високу чутливість і дозволяють визначати практично будь-які нелінійні пристрої знімання інформації, підключені до лінії. Істотним недоліком таких приладів стосовно до телефонної лінії є невелика дальність виявлення, обмежена фізичною доступністю до проводів лінії і необхідністю відключення телефонної лінії від АТС на час перевірки. Ці особливості експлуатації не дозволяють робити оперативний контроль телефонної лінії й обмежують дальність перевірки. Прилади найбільш придатні для періодичних перевірок знеструмлених відрізків ліній (телефонних, електромереж, сигналізації) у середині будинку.

Прилади, що працюють на реальній телефонній лінії (SELSP-18/Т, КТЛ-400), мають меншу чутливість у порівнянні із приладами попередньої підгрупи. Відбувається це через те, що перешкоди, спеціальні сигнали АТС, наведення промислової частоти, що є присутнім на лінії, реально не дозволяють мати таку ж чутливість. Однак їхня чутливість цілком достатня для виявлення практично всіх відомих пристроїв, що прослуховують, з живленням від телефонної лінії, що мають нелінійний характер імпедансу. З іншого боку, можливість роботи на реальній телефонній лінії, оперативність проведення контролю (не більше 5 хвилин) без порушення нормального функціонування лінії, роблять прилади другої підгрупи найбільш привабливими при експлуатації. До безсумнівних достоїнств приладів варто віднести їх багатофункціональність. Аналізатор SELSP-18/Т, виконаний як пошуковий прилад з автономним живленням, у вигляді додаткових функцій визначає "ВЧ-нав'язування" і наявність аудіосигналів на лінії.

Таким чином, можна констатувати, що на сьогоднішній день практично не існує універсальних приладів, що дозволяють однозначно визначити факт підключення до телефонної лінії. Більш того, безконтактні (індуктивні і ємнісні) знімачі без радіоканалу не визначаються жодним приладом з перерахованих груп. Варто враховувати, що найбільше практичне поширення (до 95%) мають контактні підключені пристрої прослуховування переговорів з радіоканалом і живленням від лінії і пристрою типу "телефонне вухо". Поширено прослуховування за допомогою паралельних ТА, АОНІВ і автовідповідачів. Значно більш організаційно складним, дорогим і менш

імовірним варто вважати безконтактне підключення до лінії пристроїв без радіоканалу, контактне підключення пристроїв з високим вхідним опором і зовнішнім живленням без радіоканалу, використання апаратури "ВЧ-нав'язування". Що стосується вибору з усіх вище перерахованих методів для перевірки телефонної лінії, то в кожному конкретному випадку користувач повинен виходити з того, які типи пристроїв найбільше ймовірно можуть бути підключені до лінії. Варто враховувати місце, де вони можуть бути встановлені й орієнтовна тривалість їхньої роботи. На наш погляд, найбільш ефективними в цей час є прилади радіоконтролю і прилади, що аналізують не лінійність лінії. Це викликано тим, що основна маса пристроїв для прослуховування працює з живленням від телефонної лінії (тобто містить нелінійний імпеданс) і передає інформацію в ефір, використовуючи радіоканал. Для оперативної перевірки краще використати прилади, що аналізують не лінійність імпедансу лінії. При оцінці приладів необхідно враховувати їх додаткові функції. З цієї точки зору перевагу мають методи і реальні прилади, що забезпечують функцію не лише пошуку, але й захисту переговорів по телефону. У цьому сенсі найбільш виграним з критерію "виявлення – захист" є контролер телефонних ліній КТЛ-400, який забезпечує придушення практично любых підслуховуючих пристроїв, навіть індуктивного і ємнісного типу, виявляє паралельні телефони, "телефонне вухо", "ВЧ-нав'язування" по всій довжині телефонної лінії.

4.2.2 Можливості приладу СРМ-700 «АКУЛА» у виявленні пристроїв прослуховування телефонних і інших ліній

Технічні можливості приладу СРМ-700 дозволяють проводити обстеження телефонних ліній, мереж живлення 220 В, мереж диспетчерського зв'язку і інших провідних ліній. СРМ-700 може виявити практично будь-який тип нелегального пристрою, якщо пошук за допомогою приладу доповнюється фізичним пошуком. Деякі жучки, особливо телефонні можуть працювати тільки в певний час і за певних умов. Їх, однак, можна виявити і за допомогою гарного цифрового мультиметру (тестера) з точністю вимірів 0,5% або вище.

Для прослуховування телефонних ліній використовуються в основному два типи "жучків": які включаються у лінію послідовно з телефоном або паралельно. Окрім того необхідно враховувати, що існують і безконтактні методи знімання інформації, при яких

застосовуються індуктивні і ємнісні датчики знімання. Приклади індуктивних засобів знімання інформації з телефонної лінії наведені на рис.4.1.

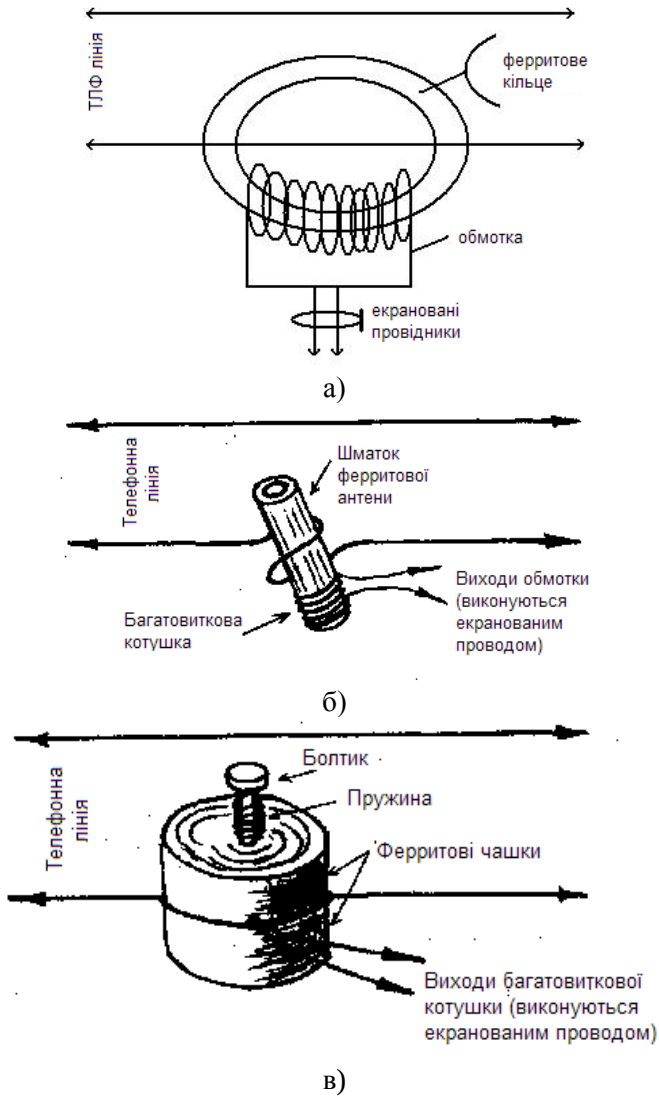


Рисунок 4.1 – Індуктивне підключення до телефонної лінії

При цьому необхідно враховувати, що лінії, у тому числі і телефонні, можуть використовуватись для знімання інформації такими методами:

- 1) Під'єднання паралельного телефонного апарата (трубки);
- 2) Встановлення прослуховуючого мікрофону, який апаратури навантажено на вільну телефонну пару з розташуванням апаратури підслуховування за межами приміщення;
- 3) Встановлення прослуховуючої закладки у мережу електроживлення 220 В;
- 4) Прослуховування приміщень за допомогою систем селекторного або диспетчерського зв'язку;
- 5) Застосування до ліній систем „ВЧ-нав'язування”;
- 6) Використання безконтактних методів знімання інформації (індуктивний або ємнісний);
- 7) Прослуховування телефонних ліній з застосуванням передавачів УКХ та інфрачервоного діапазонів.

З наведених у загальних відомостях шести принципів дії пошукових приладів СРМ-700 забезпечує два:

- Контроль навколишнього радіоефіру;
- Контроль сигналів у лінії.

4.3 Завдання на підготовку до лабораторної роботи

1. Вивчити призначення, основні технічні характеристики та принцип дії пошукового приладу СРМ-700.
2. Вивчіть опис й інструкцію з експлуатації пошукового приладу СРМ-700 та порядок роботи з ним.
3. Вивчіть теоретичний матеріал та загальні відомості наведені в методичних вказівках.
4. Ознайомтеся з порядком проведення лабораторної роботи.
5. Дайте відповідь на контрольні запитання.

4.4 Контрольні запитання для самоперевірки і контролю підготовленості студентів до роботи

1. Чому необхідно захищати телефони і телефонні лінії від несанкціонованого прослуховування?
2. Як працюють прилади контролю напруги лінії?
3. Як працюють прилади контролю навколишнього радіоефіру?
4. Як працюють прилади контролю сигналів у телефонній лінії?
5. Як працюють прилади аналізу неоднорідності телефонної лінії?
6. Як працюють прилади аналізу не симетрії лінії?
7. Як працюють прилади аналізу не лінійності параметрів лінії?
8. Які типи "жучків" можуть бути встановлені у телефонні лінії?
9. Що являють собою поширені прилади безконтактного знімання інформації?
10. Які існують методи знімання інформації з допомогою існуючих телефонних і інших ліній?
11. Які принципи контролю (пошуку) забезпечуються приладом СРМ-700?
12. Методика перевірки телефонних апаратів?
13. Як проводити перевірку розподільчих коробок та телефонних кросів?
14. Як проводити фізичний пошук?
15. Як здійснюється перевірка ліній електроживлення?
16. Як здійснюється перевірка лінійного господарства підприємств, установ на предмет виявлення каналів втрат інформації?
17. Які з каналів витоку інформації можуть використовуватись у разі наявності неконтрольованого лінійного господарства?

4.5 Матеріали, інструмент, прилади, обладнання

У якості пошукового прослуховуючого пристрою використаємо комплект СРМ-700, стетоскопу ALP-700, підключеного до додаткового входу, і головних телефонів. Можливо також скористатись низькочастотним селективним вольтметром В6-9 з мікрофоном.



Рисунок 4.2 – Вигляд передньої панелі маскувача мовних сигналів

Як джерело інформації використаємо любий малопотужний передавач, настроєний на канал мовного віщання.

4.6 Вказівки з техніки безпеки

1. По ступеню захисту від поразки електричним струмом прилади відносяться до класу захисту 01 відповідно до вимог ДСТУ 4.275.003 – 77.

2. В приладах присутня висока напруга до 220 В, небезпечна для життя, тому при експлуатації, контрольно-профілактичних та регулювальних роботах, вироблюваних з приладом, необхідно строго дотримуватися відповідних запобіжних заходів, а також перед вмиканням приймачів перевірте наявність захисного заземлення:

– до включення мережевої вилки шнура живлення необхідно перевірити справність мережевого сполучного шнура та з'єднати клеми «» приладів з шиною захисного заземлення приміщення дротом перетином жили не меншого 4 мм;

– з'єднання клеми «» з шиною захисного заземлення, провести раніше інших пристосувань до приладів, а від'єднати – після всіх від'єднань;

– у випадках використання приладів сумісно з іншою апаратурою, при проведенні вимірювань, при обслуговуванні та ремонті з'єднати клеми «» всіх приладів з шиною захисного заземлення в цілях вирівнювання потенціалів їх корпусів;

– при ремонті приладів заміну будь-якого елементу проводити тільки при вийнятій з розетки мережевої вилки шнура живлення;

– при регулюванні та вимірюваннях в схемі приладу користуватися надійно ізольованим інструментом та пробниками.

– підключення і відключення від приладу кабелю допускається проводити тільки при вимкнених кнопках «СЕТЬ».

4.7 Порядок проведення лабораторної роботи

4.7.1 Виявлення радіопередавачів

Перевірка наявності радіопередавачів у телефонних лініях і апаратах здійснюється шляхом вимірювань рівня сигналу у разі покладеної та піднятої трубки. При цьому можливо застосовувати прийом "відомого звуку", що допоможе активувати передавальні засоби і збільшити вірогідність виявлення передавача. Наявність жучка визначається прослуховуванням через навушники згідно наступної методики.

Калібрування приладу

СРМ-700 побудований на сучасній елементній базі, доповненою температурною компенсацією параметрів схеми, що забезпечує стабільну й точну роботу приладу. Через великий коефіцієнт підсилення іноді потрібна періодичне підстроювання параметрів, обумовлене старінням елементів, змін температури й вологості середовища.

Якщо ви перебуваєте в умовах не дуже інтенсивного радіополя (10 сегментів і більше при посиленні high), точне калібрування не є необхідним.

Калібрування здійснюється шляхом підключення електромагнітного зонду до зондового входу приладу з наступним настроюванням за допомогою регулятора на правому боці приладу (шліц METER) так, щоб показання дисплея становили від 2-х до 3-х сегментів при посиленні HIGH.

Самодіагностика РЧ-зонду

Чутливість РЧ-зонду може бути перевірена в умовах низького або середнього навколишнього радіовипромінювання. Для цього максимально вкоротіть антену і торкніться її кінцем шкали дисплею. Справний зонд буде видавати "шум перемикання" (добре чути гудіння),

несправний дуже тихе або взагалі не видавати, незалежно від довжини антени.

Підготовка приміщення

1. Закрийте всі вікна й фіранки для виключення візуального контакту.

2. Ввімкніть світло і всі звичайні офісні пристрої, характерні для даного приміщення.

3. Включіть джерело "відомого звуку" у центрі зони контролю для маскування процедури пошуку.

4. За межами зони контролю (у незахищеній кімнаті/зоні) як можна більш безшумно розгорніть вашу апаратуру.

5. Заміряйте звичайний рівень радіовипромінювання (фон) навколишнього середовища перед початком пошуків у зоні контролю.

РЧ-зондування

РЧ-зондування застосовується для обстеження приміщень, телефонних ліній і електропроводки на наявність несанкціонованих мікропередавачів і систем відеоспостереження.

РЧ-зонд складається з низькошумлячого зверхширокосмугового (50 кГц - 3 ГГц) підсилювача, який здатний працювати зі слабкими сигналами від мікропередавачів а також висувної антени. Рівень сигналу реєструється за допомогою дисплею в діапазонах низкої та високої чутливості. Передавач реєструється шляхом "руху в напрямку" джерела радіовипромінювання по найвищому рівню показань дисплею.

Оскільки у складі РЧ-зонду є високочутливий підсилювач, то зонд під час роботи потребує дуже обережного поводження з ним. Підсилювач може вийти з ладу від електричного розряду через антену. В умовах можливості появи статичної електрики (сухі приміщення, килими) по можливості торкніться досліджуваного об'єкта спочатку рукою, а тільки потім антеною.

Заборонено також торкатись зондом ланцюгів із включеним живленням!



Рисунок 4.3 – CPM-700 з РЧ-зондом у роботі

CPM-700 чутливий до амплітудної інформації. Деякі передавачі використовують незвичайний тип модуляції, імпульсний режим передачі даних або мають дуже вузьку смугу частот. Вони можуть не забезпечити достатнього рівня звукового сигналу і не забезпечити гарної чутності джерела "відомого звуку", а тільки зафіксувати його наявність на дисплеї. Тому уважно перевіряйте всі "підозрілі" частоти.

CPM-700 і РЧ-зонд являють собою широкосмуговий радіоприймач (50 кГц - 3 ГГц). Типові "жучки" працюють у діапазоні від 30 до 500 МГц. Більш низькі частоти потребують застосування довших антен, що не завжди можливо в реальних ситуаціях. Частоти, вищі 300 МГц, погано проходять крізь стіни будинків через відбиття й поглинання у матеріалах стін.

CPM-700 не має можливості визначати частоту виявленої радіозакладки - він лише здатний зафіксувати факт її наявності.

Починаючи пошук мікропередавачів, необхідно мати уяву про їх класифікацію. Нелегальні мікропередавачі можуть бути розділені на чотири групи: **мікропотужні, малопотужні, середньої потужності і великої потужності**. Зона приймання сигналів радіозакладок залежить не тільки від потужності, але й від форми та розташування передавальної та приймальної антен, від оточення, радіошуму і параметрів приймача. Передавачі великої потужності (більше 100 мВт) можуть передавати сигнал на відстань не меншу за 400 м. Передавачі середньої потужності мають вихідні потужності від 1 до 100 мВт і здатні працювати на

відстанях 100...400м. Малопотужні "жучки" (менше 1 мВт) передають на відстані до 100 м.

Особливу групу становлять мікропотужні передавачі, що мають потужності 1 мкВт і менше. Вони дуже малі за габаритами і мають дуже короткі антени. Для їх виявлення необхідно датчики СРМ-700 дуже близько підносити до місця розташування закладок і працювати у режимі високої (HIGH) чутливості. Через непередбачуваність ситуації в застосуванні нелегальних передавачів для їх надійності застосовується мінімально необхідна потужність.

Підключення РЧ-зонду

Наступні процедури застосовуються при кожному підключенні РЧ-зонду:

1. Підключіть головні телефони, встановіть мінімальне посилення звуку (регулятор GAIN проти годинникової стрілки).
2. Встановить перемикач режимів (Mode Switch) у позицію Search.
3. Приєднайте РЧ-зонд до зондового входу приладу (Probe) і розгорніть антену на повну довжину.
4. Включіть живлення приладу і переконайтеся в активації приладу.
5. Установіть діапазон підсилення. Якщо на дисплеї реєструється високий рівень шуму (більше 10 сегментів), то треба перемкнутися на низький (Low) рівень посилення або укоротити антену.
6. Налаштуйте підсилення звуку у головних телефонах до комфортального рівня.

Типова послідовність дій у кімнаті

1. Перед тим, як зайти до кімнати, яку необхідно обстежити, одягніть навушники і тримайте РЧ-зонд за гумову ручку перед собою у вертикальному положенні.
2. Включіть джерело "відомого звуку".
3. Входить до кімнати, коли дисплей показує середнє значення. Використовуйте діапазон підсилення "Low", якщо дисплей показує "Max" то скоротіть довжину антени.
4. Вимкніть всі прилади і світло в зоні контролю та біля неї і подивіться, чи не змінилися показання дисплея. Іноді звичайна лампа денного світла створює дуже сильне радіовипромінювання, у такому

випадку вона повинна бути виключена або вилучена з кімнати. Якщо зміни в показаннях дисплею не можуть бути викликані такими явними причинами, то це означає реальну підозру на "жучка".

5. Оберніться на 360 градусів навколо, стежачи за показаннями дисплея, вони будуть мінятися у залежності від рівня радіовипромінювання, що існує в кімнаті.

6. Виділіть напрямок з максимальним рівнем сигналу.

7. Рухаючись у цьому напрямку, обстежте всі об'єкти, у яких можуть бути заховані жучки. Якщо жучок поруч, то показання дисплея будуть зростати.

8. Інколи виявляється помилкове джерело сигналу десь у повітрі. Це означає, що реальне джерело десь поруч, тому продовжуйте пошук.



Рисунок 4.4 – Обстеження приміщення

9. Необхідно ідентифікувати виявлене джерело радіовипромінювання з метою відокремлення сигналу "жучка" від інших сигналів. За допомогою головних телефонів, ви легко визначите сигнали місцевих радіо- і TV-станцій і станцій радіозв'язку. Виявлення сигналу "відомого звуку" означає виявлення жучка.

Особливості пошуку у приміщеннях із сильним фоном

Варто помітити, що в деяких приміщеннях, близьких до потужних телевізійних- або й радіопередавачів, а також в умовах значних промислових завод навіть в умовах застосування низького підсилення "Low" показання дисплея можуть бути більше, ніж 10 сегментів.

Звичайно доводиться стежити за змінами рівня сильних сигналів. Часто, якщо зонд розташований поблизу проводів або металевго об'єкта, дисплей буде показувати збільшення рівня сигналу, так само як і звук у головних телефонах стає голоснішим. Це може означати не наявність жучка, а роботу металокопструкцій, як перевипромінюючих антен. Перевірте це за допомогою джерела "відомого звуку".

Порушники часто застосовують радіомікрофони, що працюють у комерційному FM-діапазоні. Оскільки такі передавачі працюють у частотному оточенні десятків постійно працюючих радіостанцій, то вони повинні бути відстроєними за частотою і мати вихідну потужність у декілька мікват. З цих обставин такі радіозакладки дуже важко виявляються за допомогою CPM-700. На щастя, з цих обставин такі передавачі є малоефективними через малий радіус дії, який у більшості випадків дорівнює менше 20 метрів. Тому у кожному разі необхідний ретельний фізичний пошук на додаток до CPM-700.

У місцях із сильним радіофоном CPM-700 найбільш ефективний, якщо РЧ-зонд поміщати напроти обстежуваного об'єкта і стежити, чи не перевищить показання дисплея значення фону. Варто перевіряти всі радіосигнали.

Виявлення телепередавачів

Нелегальні телепередавачі чутні в навушниках так само як і місцеві телестанції. У ряді випадків можна порівняти рівень сигналу зображення і каналу звуку, просто перемістившись в іншу кімнату. Якщо ви помітили, що зміни освітленості у приміщенні приводять до змін і тону і рівня сигналу, то визначте область із найбільшими показаннями дисплею і шукайте передавач або камеру.

4.7.2 Порядок перевірки телефонних апаратів і телефонної лінії

Викладена нижче методика дозволяє здійснити перевірку телефонних апаратів та ліній зв'язку на предмет наявності паралельно підключених апаратів з системою "Vox" та "ефекту нав'язування".

1. Включіть CPM-700 з РЧ-зондом у режимі високої чутливості приладу з роботою на навушники.

2. Наблизьте зонд до телефону на відстань приблизно 10 см для зменшення впливу навколишнього радіофону та відрегулюйте СРМ-700.

3. Порівняйте рівні сигналів в кімнаті та поблизу телефону у випадках покладеної і піднятої трубки. Якщо реєструється помітне збільшення показань дисплея, те необхідно перевірити по прийнятому звуковому сигналу, це легальний сигнал (швидше за все короткохвильовий або найближчої FM-станції) чи мікропередавач, який живиться від телефонної лінії.



Рисунок 4.5 – Перевірка телефонного апарату з допомогою РЧ-зонду

4. Намотайте не менше ніж чотири оберти проводу від слухавки навколо антени і повторіть вимірювання згідно п.2 (рис.4.5).

5. Відзначивши поточні показання дисплея, підійміть слухавку і стежте за змінами показань (нормальне збільшення на два сегменти). Прослухайте набір номера через навушники. Якщо збільшення показань відбувається, а через навушники прослуховується сигнал, то це говорить про можливу присутність передавача. "Чистий" телефон робить усього лише неголосний короткий звук і стрибок показань дисплея. Здійсніть перевірку шляхом застосування „відомого звуку”.

6. Перевірте телефон, повторивши вищеописані процедури, пересуваючи зонд навколо телефону, виміряйте різницю показань при піднятій і опущеній трубці. Прослуховуйте тон набору.

7. Перевірте лінію в тім місці, де вона входить у стіну або у розетку, повторивши підняття/опускання трубки (рис.4.6).



Рисунок 4.6 – Перевірка телефонної лінії

8. Аналогічним чином перевірте розподільчу коробку. Хто-небудь повинен у цей час піднімати й опускати трубки.

9. Те ж саме проробіть із місцем, де телефонна лінія входить в зовнішню стіну споруди.

10. Повторіть всі вимірювання, але з допомогою ОНЧ-зонду.

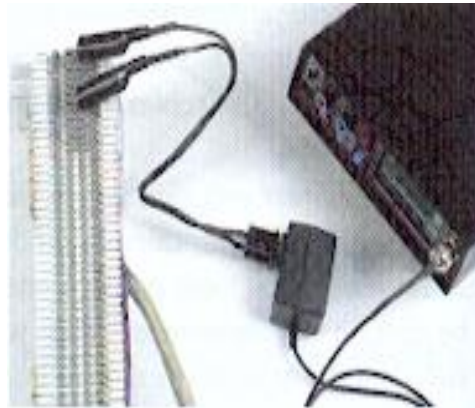
11. Визначте телефонні проводники для живлення телефону (звичайно червоний і зелений) і приєднайте до них кабель додаткового входу CRM-700 (на правій стороні приладу). ВЧ-зонд при цьому необхідно відключити.

12. Прослухайте через навушники сигнал від джерела "відомого звуку"- "чистий" телефон не транслює звук при лежачій трубці. Якщо на лінії є "електронний тригер" або в телефоні встановлено перемиčku для активізації мікрофона при лежачій трубці, то ви почуєте в навушниках ваш звук. У цьому випадку перевірте лінію і телефонний апарат на наявність жучків.

13. Повторіть цей тест із кожною комбінацією проводів, з'єднаних з телефоном. При необхідності перевірте призначення кожного провідника за допомогою цифрового вольтметра.

4.7.3 Перевірка розподільчих коробок та телефонних кросів

У комплект СРМ-700 входить необхідне додаткове обладнання, яке дозволяє провести оперативне під'єднання до ламелей кросу, до проводників ліній. Для цього використовуються два різновиди проводників, що мають на своїх кінцях з'єднувачі типу "крокодил", а до іншого кінця приєднана або розетка або штекер для НЧ-входу (див. рис.4.7).



а)



б)

Рисунок 4.7 – Перевірка телефонних ліній на наявність ВЧ-нав'язування (а) та на наявність прослуховування (б)

Слід враховувати, що з допомогою НЧ-входу (на правій боковій панелі СРМ-700) здійснюється безпосереднє прослуховування ліній. **При цьому напруга у таких лініях не повинна перевищувати 50 В!** (рис. 4.7 б).

Приклад перевірки ліній на кросі АТС на предмет виявлення ефекту ВЧ-нав'язування наведено на рис. 4.7 а. Для цього використовується додатковий шнур з розеткою та "крокодилами" і фільтр-приймач VLF-700 (рис. 4.7 а).

4.7.4 Фізичний пошук

1. Перевірку телефонних ліній за допомогою приладу необхідно доповнити фізичним пошуком. Варто розібрати телефонний апарат і розетки й шукати несхожі на звичайні телефонні деталі з різнобарвними проводами й спішною або неакуратною установкою.

2. Перевірте лінію від апарата до стіни, видаліть стінну панель, перевіряючи всі нестандартні деталі.

3. Проведіть фізичний пошук у комутаційних панелях та у кросі.

4. Проведіть фізичний пошук у місцях входу/виходу проводів усередині й зовні будинку.

4.7.5 Перевірка ліній електроживлення

Як було вказано вище, мережа електроживлення також може використовуватись для знімання звукової інформації з приміщень. При цьому НЧ безпосередньо транслюється по мережі 220 В. Передавач монтується у розетці або у розподільчій коробці. Він живиться від напруги електромережі і являє собою резистивний подільник напруги, випрямляч, фільтр і підсилювач з якісним мікрофоном. Для захисту схеми від високої напруги використовується високовольтні розділові конденсатори. Приймач також включається у розетку електроживлення, але у іншому приміщенні. Приймач являє собою фільтр НЧ і якісний підсилювач НЧ з схемою електроживлення. Схема також захищається від високої напруги електромережі з допомогою конденсаторів.

Для перевірки включіть СРМ-700 з фільтром-приймачем сигналів з мережі електроживлення VLF-700 (рис. 4.8) і послідовно вставте фільтр у всі розетки, що розташовані у кімнаті.



Рисунок 4.8 – Фільтр-приймач VLF-700



Рисунок 4.9 – Тестовий передавач для передачі сигналів по мережі живлення CCT-700

Під час виконання цієї частини лабораторної роботи можна застосовувати тестовий передавач для мережі електроживлення CCT-700. Його можна вставити у розетку у лабораторії або у сусідньому приміщенні. Необхідно перевірити, щоб лінія електроживлення, у яку встановлено передавач і приймач, була утворена однією і тою ж фазою.

4.7.6 Перевірка лінійного господарства

У разі довгострокової експлуатації споруд у коридорах і багатьох приміщеннях накопичується багато старих вільних телефонних пар і інших провідних ліній. Ці провідні лінії можуть використовуватись також для завдань несанкціонованого знімання звукової інформації. Тому проводячи обстеження приміщень виявіть, які з ліній вже не використовуються за своїм прямим призначенням і обов'язково обстежте їх приладом CPM-700. Для обстеження застосовуйте ВЧ-зонд, ОНЧ-зонд, фільтр-приймач VLF-700, а також НЧ-вхід з комплектом проводів, які мають штекерний роз'єм і "крокодили" для приєднання до лінії.

НЧ-вхід слід використовувати дуже обережно, оскільки без контролю тестером рівня напруги у лініях, можна вивести з ладу весь прилад.

Напруга у лініях, що контролюються, не повинна перевищувати 50 В!

Навіть якщо лінія використовується легально, те це не виходить, що вона безпечна з погляду витоку інформації. Гучномовці, інтеркоми, комп'ютери, радіоприймачі і охоронна сигналізація, що реагує на звук, можуть бути використані для нелегального прослуховування приміщення. Коли гучномовець видає звук, те звичайно він не може працювати як мікрофон, але якщо він виключений, то безумовно може.

Щоб застрахувати себе від цього, від'єднайте і винесіть всі гучномовці, що не використовуються в цій кімнаті. Із тими, що залишилися варто поступити таким чином: або закоротіть кожен динамік з метою фізичної ізоляції гучномовця, або встановіть схему, яка замість замість динаміка буде вмикати резистор з опором, що дорівнює опорі катушки динаміка.

Варто проявити обережність при роботі з компанією, що встановлює охоронну сигналізація в офісі, яка працює за допомогою прослуховування внутрішніх ліній, контролюючи в такий спосіб що відбувається в приміщеннях офісу. Хоча більшість компаній заслуговують довіри, факти несанкціонованого прослуховування існують. Навіть якщо охоронна система відключається в робочий час, лінія з мікрофоном залишається на місці й може бути використана для нелегального прослуховування.

У залежності від необхідного рівня безпеки іноді має сенс не обладнувати приміщення типу конференц-залу охоронною сигналізацією, що контролює звук в приміщенні.

4.8 Зміст звіту

1. Обґрунтуйте задачі і параметри отримані під час дослідження.
2. Наведіть основні алгоритми маскування мовних сигналів у каналах зв'язку.
2. Наведіть рівні при яких визначити закладний пристрій стає неможливо в кожному дослідженні.
3. Опишіть суб'єктивні відчуття прослуховування сигналу закладного пристрою на різних відстанях.

4.9 Рекомендована література

1. CPM-700: Countersurveillance Probe/Monitor. Manual contains proprietary information intended solely for use with the CPM-700 and CPM-700 Probes and Accessories: Research Electronics International, USA.
2. Остапов С.Е. Технології захисту інформації: навчальний посібник [Текст] / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
3. Жилін А.В. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. [Текст] / А.В. Жилін, О.М. Шаповал, О.А. Успенський; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
4. Бурячок В.Л. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. [Текст] / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко. – К.:ДУТ, 2015. – 345 с.

5. ЛАБОРАТОРНА РОБОТА №5. ДОСЛІДЖЕННЯ ГЕНЕРАТОРУ АКУСТИЧНОГО ЗАШУМЛЕННЯ ANG-2200

5.1 Мета роботи

Метою лабораторної роботи є перевірка властивостей та здатності комплексу ANG-2200 створювати завади, які перекривають акустичний канал витоку розмовної інформації.

5.2 Загальні відомості

Інформація, яка передається усно співрозмовнику, являє собою високу цінність з таких обставин:

- Усно передають відомості, які інколи не можуть бути довірені навіть технічним засобам передачі;
- Інформація, отримана в момент її озвучування, є самою оперативною;
- Сучасні методи обробки аудіозапису дають можливість ідентифікувати особистості тих, хто вів розмову.

Такі особливості пояснюють неослабний інтерес до безпосереднього підслуховування розмов. Для захисту розмов від несанкціонованого прослуховування застосовуються пасивні і активні методи. Пасивні методи призводять до ослаблення акустичних сигналів, що циркулюють у приміщенні, а також продуктів електроакустичних перетворень у лініях, що виникають як природним шляхом, так і в результаті ВЧ-нав'язування.

Активні методи передбачають створення штучних шумових завад, що маскують розмову, придушують апарати звукозапису і пристрої для підслуховування, а також здійснюють знищення закладних пристроїв.

Ця лабораторна робота присвячена вивченню сучасного генератора активного зашумлення акустичного каналу можливого витоку інформації типу ANG-2200.

5.2.1 Призначення генератору ANG-2200

Генератор ANG-2200 є представником сучасної апаратури забезпечення активного захисту технічних каналів витоку акустичної інформації. При цьому захист здійснюється шляхом утворення шумової

завади за допомогою як динамічних гучномовців, так і за допомогою віброакустичних перетворювачів (БАП). ANG-2200 розроблено і виготовлено фірмою Research Electronics, Intl. (REI), США. Аббревіатура ANG означає Akustik Noise Generator – Генератор Акустичних Шумів.

Коливання повітря, які викликані розмовами у приміщенні, можуть бути передані вентиляційними каналами, іншими технологічними отворами, трубами будівельних комунікацій, стінами, стелями, і т.п. Ці коливання можуть бути зареєстровані і прослухані на деякій відстані від джерела. А це означає, що навіть у разі, коли приміщення було очищене від підслуховувальних пристроїв, мовна інформація залишається вразливою.

Цей генератор здійснює акустичне зашумлення периметру робочого приміщення, а також зашумлення будівельних конструкцій з метою ліквідації або суттєвого ослаблення акустичного та віброакустичного каналів витоку інформації. ANG-2200 захищає від можливостей прослуховування за допомогою мікрофонів (як вбудованих, так і у складі радіозакладних пристроїв), а також лазерно-мікрохвильових пристроїв знімання інформації з вікон та віддзеркалюючих поверхонь.

5.2.2 Принцип дії та технічні характеристики генератору ANG-2200

Захист акустичної інформації здійснюється за допомогою джерел штучного шуму, які накладають на розмовний сигнал нефільтруємий шум. ANG-2200 являє собою двоканальну конструкцію генератору випадкових шумів з двома ідентичними каналами. До складу генератору входить комплект із трьох гучномовців OMS-2000, віброакустичний перетворювач TRN-2000, блок електроживлення. Такий комплект дозволяє більш точно вивчити маскуючі властивості розмов ANG шляхом регулювання необхідного рівня акустичного та віброакустичного зашумлення. При цьому зашумлення об'єму приміщення здійснюється за допомогою системи гучномовців, а зашумлення віброакустичних каналів витоку інформації – за допомогою віброакустичних перетворювачів. Таким чином можливо захищати як периметр, так і об'єм приміщення.

Розділене зашумлення з двома окремими каналами дозволяє більш точно реалізувати задачу постановки завад і мати більш комфортні умови для повсякденної роботи працюючих у захищеному приміщенні, тому що тут утворюється розподілене і спрямоване зашумлення з невисоким рівнем механічних шумів, які виникають за рахунок механічних коливань віброакустичних перетворювачів, а також динаміків. Перетворювачі забезпечені системами кріплення до різних будівельних конструкцій.

Система ANG 2200 захищає периметр приміщення, шляхом утворення звукового бар'єру, який і є перепорою на шляху витоку розмовної інформації. Перетворювачі TRN-2000 призначені для утворення маскуючих шумів на огорожувальних поверхнях контрольованого приміщення, в той час як гучномовці OMS-2000 використовуються з метою захисту повітряного простору того ж об'єму, та того, що вище підвісної стелі. Такий метод забезпечує утворення маскуючої „шумової ковдри” для контрольованого приміщення.

Спектр утворюваного шуму розподілений за нормальним законом у діапазоні мовних частот. Вигляд гістограми розподілу спектральної щільності генерованих шумів наведено на рис.5.1.

ANG-2200 створений для завдань захисту від пристроїв, які можуть бути не виявлені у процесі фізичних або радіотехнічних пошуків.

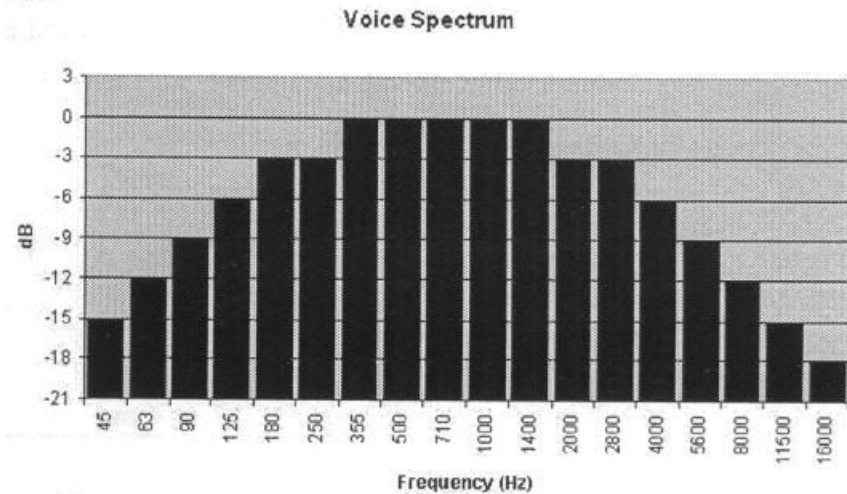


Рисунок 5.1 – Гістограма розподілу спектральної щільності шуму

Характеристики ANG-2200

Розміри	20,3 x 14,0 x 4,1 см
Маса	0,5 кг
Кількість каналів	2
Вихідна напруга	змінна 0-14 В на 6 Ом
Мінімальне навантаження	2 Ом
Діапазон робочих частот	125 Гц - 4 кГц, +/- 3 dB
Живлення	DC $\pm$ 12V, 1A

Віброакустичний перетворювач TRN-2000

Розміри	Ø101.6 x 38.1 мм
Маса	454 г.
Опір	6 Ом

Гучномовець OMS-2000

Розміри	12,7 x 14,6 см
Маса	907 г.
Опір	24 Ом

Блок живлення

AC $\approx$ 220 V, 50/60 Гц; DC $\pm$ 14...16V, 1...2A, 25 Вт.

Система ANG-2200 утворює звукові хвилі у об'ємі приміщень і визиває вібрації їх огорожувальних поверхонь, таких як стіни, вікна, двері, стіни, підлоги. Адже для прослуховування акустики приміщень можуть використовуватись як акустичні, так і віброакустичні мікрофони, а також лазерні, інфрачервоні або мікрохвильові промені, що відбиваються від різних відбивих поверхонь безпосередньо розташовані у об'ємі приміщень.

Як відомо, звуки можуть поширюватись у різних матеріалах зі швидкістю, більшою, ніж у повітрі. Пристрої підслуховування використовують ці якості будівельних матеріалів і конструкцій за допомогою контактних мікрофонів – фонендоскопів або акселерометрів. Такі мікрофони реєструють вібрації труб, будівельних конструкцій, стін, вікон, дверей, підлоги, стелі і т.і. Завдяки поширенню віброакустичних хвиль мікрофон може не знаходитись у тій кімнаті, де відбувається розмова, а може бути механічно під'єднаним до елементів будівельних конструкцій або інженерних комунікацій на відстані декількох поверхів або кімнат.

Встановлені у приміщеннях проводні мікрофони виявляються дуже важко, оскільки навкруги них не утворюються ніякі характерні фізичні ефекти. Такі мікрофони, за звичай, ховаються у стінах, у меблях або за плінтусами, у приладах освітлення. ANG-2200 здатний нейтралізувати такі пристрої.

Структурну схему пристрою для технічної реалізації генераторів акустичних завад для захисту каналів витоку мовної інформації наведено на рис. 5.2.



1 - генератор білого шуму; 2 -смуговий фільтр; 3 - октавний еквалайзер; 4- підсилювач потужності; 5- система перетворювачів (акустичні колонки, віброперетворювачі)

Рисунок 5.2 – Технічна реалізація активних методів захисту розмовної інформації

Задаючий генератор (генератор «білого шуму») у ANG-2200 реалізовано на основі цифрового генератору псевдовипадкових чисел.

5.2.3 Робота з генератором

Генератор ANG-2200 застосовується для захисту виділених приміщень. До початку встановлення генератора необхідно обов'язково провести обстеження такого приміщення з метою виявлення можливих закладок. Таке обстеження можливо провести, наприклад, за допомогою зонду-монітору СРМ-700 ("Акула").

Основне призначення ANG-2200 – забезпечити надійний захист периметру виділеного приміщення. Тому розташовані в центрі кімнати або на робочому місці співробітника підслуховуючі пристрої можуть виконати свою роль.

5.2.3.1 Розрахунок необхідної кількості перетворювачів

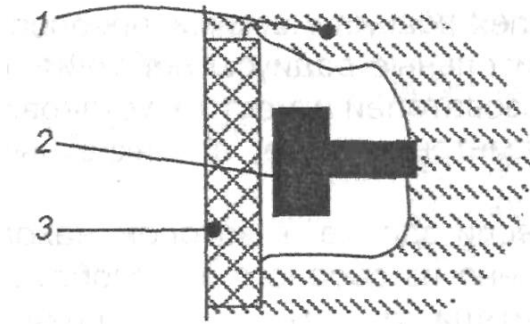
Фірма-виготовлювач рекомендує визначати необхідну кількість перетворювачів з таких міркувань:

- Стіни: 1 на кожні 3 метра довжини, по центру між підлогою і стелею;

- Підлога або стеля: 1 на кожні 9 кв.м.
- Вікна: 1 на кожну віконну раму по її центру:
- Двері: 1 на кожні двері (встановлювати посередині верхньої частини дверної коробки).

5.2.3.2 Особливості монтажу віброакустичних перетворювачів

Ідеальним випадком організації активного захисту приміщення є встановлення системи зашумлення на етапі будівництва або реконструкції. Вразливі ділянки приміщення можуть бути захищені віброперетворювачами, вбудованими у споруду. У разі можливості вони монтуються безпосередньо на стіни і стелю. Перетворювачі можуть поміщатись у спеціальні заглиблення у стінах, отвори яких закриваються кришкою з гіпсокартону, як це показано на рис. 5.3.



1— основна будівельна конструкція; 2- перетворювач; 3- кришка з гіпсокартону

Рисунок 5.3 – Монтаж віброперетворювача

Комплект поставки ANG-2200 має 3 основні монтажні елементи:

- прямий гвинт: для твердих поверхонь (дерево, цегляна кладка, лита стіна – з попереднім встановленням пробки-дюбеля);
- пластиковий спеціальний диск: для кріплення за допомогою трьох гвинтів до дерев'яних або до капітальних стін, стель, підлог;
- плівка (міцний папір), яка з двох боків покрита клеючим шаром – для встановлювання перетворювачів на площинних рівних поверхнях (скло, пластик і т.п.)

У разі постійної установки перетворювачів на скло або іншу подібну поверхню слід скористатись силіконовим клеєм для зовнішніх

робіт. При цьому така суміш наноситься на центр перетворювача, який потім щільно притискається до поверхні з тим, щоб уникнути появу повітряних кульок. У цьому стані перетворювач утримується до повного затвердіння клею (згідно інструкції на клей).

Рекомендується встановлювати перетворювачі перед під'єднанням проводки. Це запобігає непотрібному закручуванню проводів.

Динаміки OMS-2000 кріпляться шляхом підвішування за з'єднувальний провід на необхідній висоті.

5.2.3.3 Підключення перетворювачів і динаміків

Забороняється вмикання генератору без навантаження!

Існують різноманітні варіанти підключення як вібродатчиків TRN-2000, так і динаміків OMS-2000. Слід пам'ятати основне правило: **навантаження в кожному каналі не повинно мати опір, менший за 2 Ом.**

Фірма-виробник ANG-2200 пропонує керуватись такими поняттями:

- «Повний рівень потужності» ("Full Level")- це рівень, який необхідно забезпечити для віброзашумлення стін, підлоги і стелі;
- Для віконного скла, тонких перегородок для кожного перетворювача (датчика) необхідно забезпечувати рівень у 2 або 3 рази менший ("1/2 Level" або "1/3 Level").

Опір навантаження R_n розраховується за звичайною методикою:

-для послідовних кіл

$$R_n = R_1 + R_2 + \dots R_n,$$

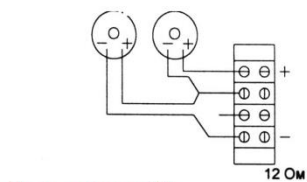
а для паралельного з'єднання опорів двох навантажень:

$$R_i = \frac{R_1 \cdot R_2}{R_1 + R_2}.$$

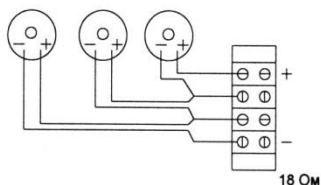
Монтаж слід виконувати проводом, загальний опір якого не повинний перевищувати 4 Ом. У випадках великих відстаней від генератора до перетворювача необхідно використовувати узгоджувальний (підвищуючий) трансформатор $\approx 15V$: $\approx 70V$.

Під'єднання слід виконувати шляхом пропаявання або обжимання проводу навколо клем перетворювача.

На наведених нижче рисунках показано різноманітні варіанти з'єднань віброакустичних перетворювачів для реалізації різних рівнів потужності- "Full", "1/2" і "1/3".

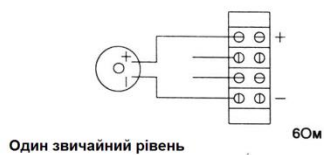


Рівень на датчику 1/2

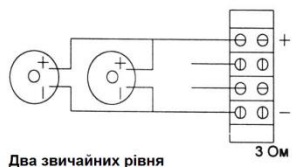


Рівень на датчику 1/3

Рисунок 5.4 – Послідовне з'єднання перетворювачів



Один звичайний рівень



Два звичайних рівня



Три звичайних рівня



Чотири звичайних рівня

Рисунок 5.5 – Паралельне з'єднання перетворювачів

За звичай дотримуються таких правил: послідовне з'єднання використовується для зашумлення вікон, а паралельне – для захисту стін, стель, підлог, дверей, але це не є догмою.

Не припустимо підключати більше 4-х перетворювачів у разі їх паралельного включення, оскільки опір буде дуже малим і це може призвести до виходу з ладу генератора. Ознакою перевантаження в будь-якому з каналів є загоряння червоного сегменту, який розташовано в кінці шкали відповідного індикатору.

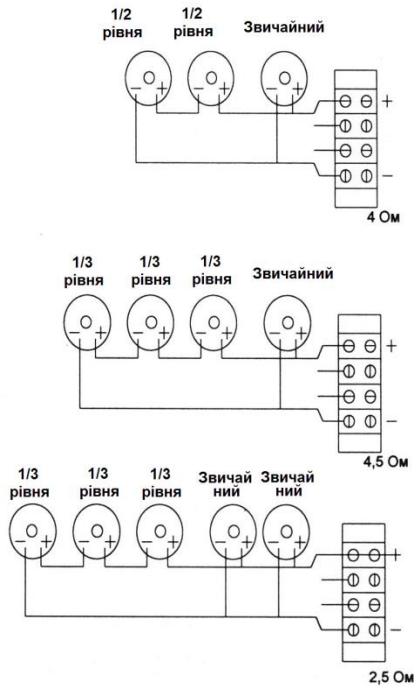


Рисунок 5.6 – Змішане з'єднання перетворювачів

На рис.5.7 наведено три можливі комбінації з динаміків OMS-2000. Рівень "Full" рекомендується для великих туалетів і комор, рівень "1/2" використовується для невеликих комор, туалетів і підвісних стель зі значною відстанню між підвісною конструкцією і самою стелею. Рівень "1/3" використовується для маленьких приміщень і малих відстаней між підвісною конструкцією і стелею.

На рис. 5.8 наведено варіант розташування обладнання кімнати переговорів і приклад розміщення у ній перетворювачів TRN-2000 і динаміків OMS-2000. Як видно на верхній частині рисунку, зліва і справа від кімнати переговорів розташовано по три приміщення. Тому, не дивлячись на те, що для такого розміру стіни було б достатньо і одного перетворювача, але з врахуванням важливості такого приміщення для віброзашумлення стін, що розділяють кожену кімнату застосовано додатково по одному віброперетворювачу. Загальна кількість віброперетворювачів у цій кімнаті дорівнює 11, а кількість гучномовців – двом. Схему з'єднання зашумлюючих елементів наведено на нижній частині рисунку.

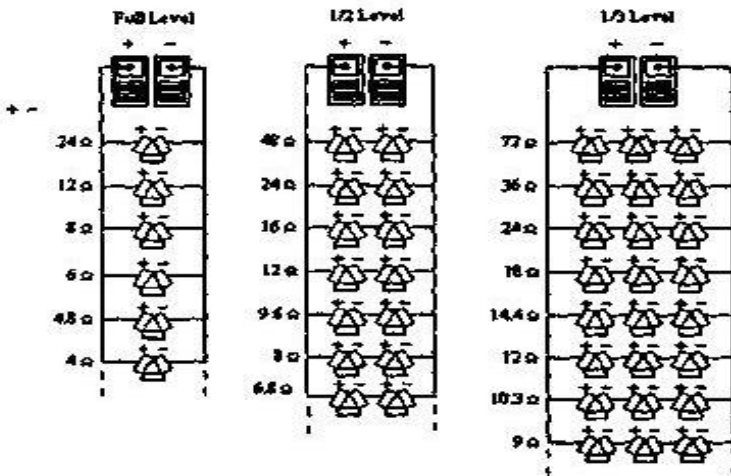


Рисунок 5.7 – Варіанти підключення гучномовців для досягнення різних рівнів зашумлення

5.2.3.4 Установлення необхідного рівня сигналу

Необхідний рівень шуму, який потрібний для маскування розмовних частот, залежить від розмірів площі, сполучення різних видів поверхонь, зовнішніх шумів і загальної гучності розмов, які необхідно маскувати. У більшості практичних випадків необхідно застосовувати "помірний" рівень шумів, який дозволяє вільно вести розмову у приміщенні. Взагалі, рівень сигналу від генератору повинний перевершувати рівень розмовного сигналу на 20 дБ.

Згідно рекомендацій фірми-виробника необхідно встановити такі рівні сигналів:

- "8" сегментів для рівня "Full";
- "6" сегментів для рівня "1/2";
- "3" сегменти для рівня "1/3".

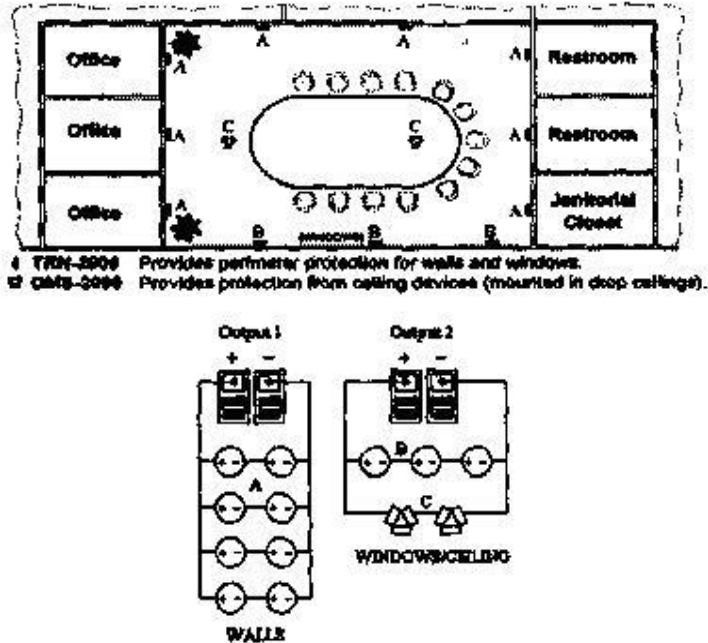


Рисунок 5.8- Варіант розташування перетворювачів і динаміків у разі захисту кімнати переговорів за допомогою ANG-2200

Встановлення необхідного спектру частот здійснюється за допомогою регуляторів НЧ і ВЧ. Але щоб досягти необхідного розподілу генерованих частот, треба скористатись аналізатором спектру і якісним мікрофоном. Необхідно досягти вигляд спектральної характеристики, близький до представленого на рис. 5.1. У разі відсутності вимірювальної апаратури, слід поставити регулятори НЧ та ВЧ у середні положення.

Фірма-виробник продає чотири різновиди додаткових резисторів до ANG-2200. Їх опір дозволяє встановити необхідний рівень сигналу у разі

використання різної кількості перетворювачів TRN-2000 і динаміків OMS-2000. Величини опорів дорівнюють: 6 Ом, 12 Ом, 24 Ом, 48 Ом.

В цілях перевірки якості захисту бажано на кожному конкретному об'єкті провести вимірювання за допомогою вимірювального мікрофону, високоякісного підсилювача і навушників, наприклад, вимірювального приладу EAR-200 (фірми REI). Таким комплексом із застосуванням "джерела відомого звуку" необхідно перевірити можливість розпізнавання окремих слів і речень.

5.3 Завдання на підготовку до лабораторної роботи

1. Вивчити призначення, основні технічні характеристики та принцип дії генератору ANG-2200.
2. Вивчіть структурну схему лабораторної установки (рис.5.9), а також передню та задню панелі (рис.5.10 – 5.11) для дослідження роботи генератора.
3. Вивчіть опис й інструкцію з експлуатації генератора ANG-2200 та порядок роботи на ньому.
4. Вивчіть опис й інструкцію з експлуатації віброакустичного перетворювача TRN-2000 та порядок роботи з ним.
5. Вивчіть опис й інструкцію з експлуатації гучномовців OMS-2000 та порядок роботи з ними.

5.4 Контрольні запитання для самоперевірки і контролю підготовленості студентів до роботи

1. Основне призначення генератору ANG-2200?
2. Що входить до комплекту ANG-2200?
3. Що складає цінність розмовної інформації?
4. За рахунок яких елементів будівельних конструкцій утворюються канали витоку мовної інформації?
5. У чому різниця між акустичними і віброакустичними каналами витоку інформації?
6. Основні характеристики робочого блоку генератора ANG-2200
5. Параметри віброакустичного перетворювача TRN-2000?
8. Параметри колонки гучномовців OMS-2000?
9. Параметри блока живлення?

10. Проти яких каналів знімання мовної інформації ефективно працює ANG-2200.

11. Типова структурна схема генераторів шуму і який тип задаючого генератора використовується у ANG-2200? Які пристрої можуть використовуватись у каскаді задаючого генератору?

12. Яким чином утворюється маскуюча «шумова ковдра» у контрольованому приміщенні? Принцип її дії?

13. Що захищає ANG-2200 об'єм приміщення чи його периметр?

14. За рахунок чого робота перетворювачів супроводжується механічними шумами і як вони діють на співробітників, які працюють у виділеному приміщенні?

15. Яким чином кріпляться віброперетворювачі до елементів будівельних конструкцій? Які базові елементи входять до комплексу ANG-2200?

16. Яке існує основне правило під час розрахунків сумарного навантаження для генератору ANG-2200?

15. Які поняття запропоновані фірмою-виробником ANG-2200 для характеристики рівнів утворюваних шумів? Для захисту яких будівельних конструкцій застосовуються ці рівні?

18. За якою схемою забезпечується рівень "1/2" для віброперетворювачів TRN-2000, а опір навантаження дорівнює 6 Ом?

19. За якою схемою забезпечується рівень "1/3" для віброперетворювачів TRN-2000, а опір навантаження дорівнює 4,5 Ом?

20. За якою схемою забезпечується рівень "Full" для колонок динаміків OMS-2000, а опір навантаження дорівнює 6 Ом?

21. За якою схемою забезпечується рівень "1/2" для колонок динаміків OMS-2000, а опір навантаження дорівнює 12 Ом?

22. Наведіть приклад змішаної схеми, коли в канал включено і перетворювачі і гучномовці, а опір навантаження дорівнював близько 13 Ом?

23. За якою схемою можливо здійснити акустичний захист однієї з кімнат вашої квартири?

24. За якою схемою можливо здійснити акустичний захист аудиторії № 38?

5.5 Матеріали, інструмент, прилади, обладнання

У якості прослуховуючого пристрою використаємо комплект СРМ-700 у складі самого приладу, стетоскопу ALP-700, підключеного до додаткового входу, і головних телефонів. Можливо також скористатись низькочастотним селективним вольтметром В6-9 з мікрофоном.

Як джерело звуку використаємо транзисторний приймач, настроєний на канал мовного віщання.

Функціональна схема лабораторної установки і робочого місця наведена на рис. 5.9.

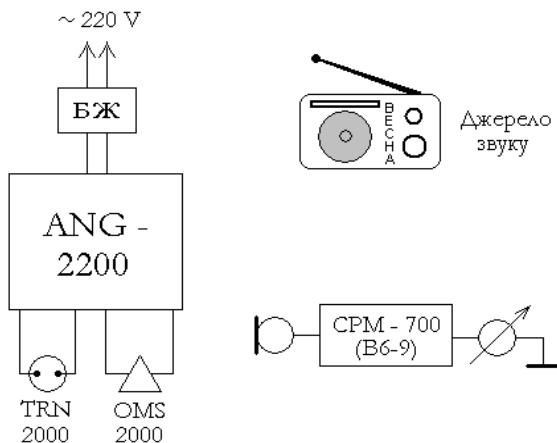


Рисунок 5.9-Схема лабораторної установки

На рис. 5.10 наведено вигляд передньої панелі ANG-2200.

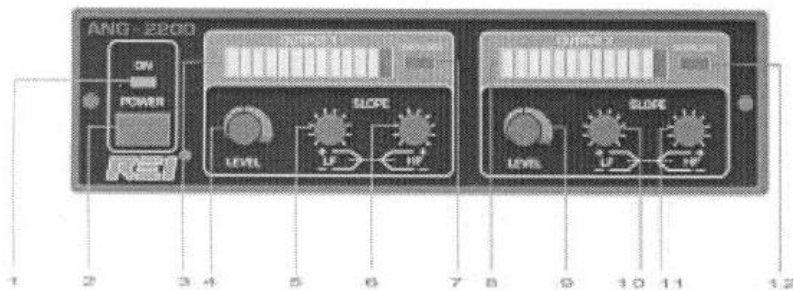


Рисунок 5.10- Вигляд передньої панелі ANG-2200

1. Індикатор вмикання
2. Кнопка включення живлення
3. Індикатор вихідного рівня каналу-1
4. Регулювання рівня вихідного сигналу каналу-1
5. Регулятор НЧ каналу-1
6. Регулятор ВЧ каналу-1
7. Індикатор перевантаження каналу-1
8. Індикатор вихідного рівня каналу -2
9. Регулювання рівня вихідного сигналу каналу -2
- 10.Регулятор НЧ каналу-2
- 11.Регулятор ВЧ каналу-2
12. Індикатор перевантаження каналу -2

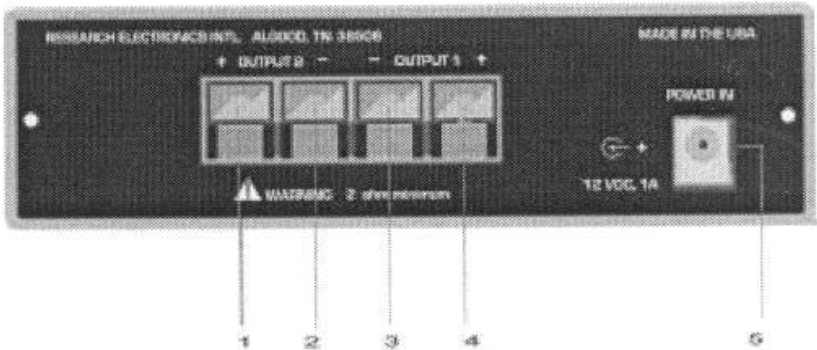


Рисунок 5.11- Вигляд задньої панелі ANG-2200

- 1.Позитивний (+) рознім виходу генератора- 2
- 2.Негативний (-) рознім виходу генератора- 2
- 3.Позитивний (+) рознім виходу генератора- 1
- 4.Негативний (-) рознім виходу генератора- 1
- 5.Підключення постійного струму $\pm 12V$, 1A від блоку живлення.

5.6 Вказівки з техніки безпеки

1. В приладах присутня висока напруга до 220 В, небезпечна для життя, тому при експлуатації, контрольно-профілактичних та регулювальних роботах, вироблюваних з приладом, необхідно строго

дотримуватися відповідних запобіжних заходів, а також перед вмиканням приймачів перевірте наявність захисного заземлення:

– до включення мережевої вилки шнура живлення необхідно перевірити справність мережевого сполучного шнура та з'єднати клеми «» приладів з шиною захисного заземлення приміщення дротом перетином жили не меншого 4 мм;

– з'єднання клеми «» з шиною захисного заземлення, провести раніше інших пристосувань до приладів, а від'єднати – після всіх від'єднань;

– у випадках використання приладів сумісно з іншою апаратурою, при проведенні вимірювань, при обслуговуванні та ремонті з'єднати клеми «» всіх приладів з шиною захисного заземлення в цілях вирівнювання потенціалів їх корпусів;

– при ремонті приладів заміну будь-якого елемента проводити тільки при вийнятій з розетки мережевої вилки шнура живлення;

– при регулюванні та вимірюваннях в схемі приладу користуватися надійно ізольованим інструментом та пробниками.

– підключення і відключення від приладу кабелю допускається проводити тільки при вимкнених кнопках «СЕТЬ».

2. Не підключайте паралельно більше трьох перетворювачів TRN-2000 з тим, щоб опір навантаження був не менше 2 Ом;

3. Не допускайте ударів та падіння генератору.

5.7 Порядок проведення лабораторної роботи

Експериментальна частина

Зберіть схему лабораторного стенду згідно рис. 5.9 (тут БЖ- блок живлення). Джерело звуку розташуйте на відстані 1...2 м від мікрофону (стетоскопу).

Проведіть наступні дослідження:

- Підключіть до одного з каналів генератору ANG-2200 віброакустичний перетворювач TRN-2000, а до іншого - динаміки OMS-2000. Перетворювач закріпіть на спеціальному пластиковому кріпленні з комплекту ANG-2200. **Вмикати генератор без навантаження заборонено!**

- Включіть джерело звуку. За допомогою головних телефонів комплекту CPM-700 або B6-9 визначте розбірливість і гучність звуку у разі покладеного на стіл стетоскопу.
- Розташуйте на столі, де розташовано стетоскоп, віброакустичний перетворювач TRN-2000 (кріпленням донизу) і поряд розташуйте динаміки OMS-2000. Перевірте, щоб регулятори рівнів виходу на обох каналах ANG-2200 знаходились у лівому крайньому положенні (мінімум). Ввімкніть генератор ANG-2200.
- Збільшуйте рівень сигналу у каналі перетворювача TRN-2000 і визначте той рівень сигналу, при якому розбірливість звуку у головних телефонах стає нульовою. Рівень сигналу визначаєте за 10-сегментним індикатором каналу. Налаштуйте на мінімум регулятор рівня сигналу цього каналу.
- Проведіть аналогічне дослідження для колонки гучномовців OMS-2000.

Обробка результатів досліджень

- Порівняйте маскуючі властивості TRN-2000 і OMS-2000.

5.8 Зміст звіту

1. Обґрунтуйте задачі і параметри отримані під час дослідження.
2. Наведіть рівні при яких розбірливість звуку стає нульовою в обох дослідженнях.
3. Наведіть графіки зміни рівня сигналу визначеним за 10-сегментним індикатором каналу при використанні у каналі перетворювача TRN-2000 та для колонки гучномовців OMS-2000.

5.9 Рекомендована література

1. ANG-2200. Acoustic Noise Generator/ Owner's Guide. Research Electronics. Intl., USA. 2005.-19 p.
2. Остапов С.Е. Технології захисту інформації: навчальний посібник [Текст] / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
3. Бурячок В.Л., Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. [Текст] / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко. – К.:ДУТ, 2015. – 345 с.

6 ЛАБОРАТОРНА РОБОТА №6. ДОСЛІДЖЕННЯ МАСКУВАЧА МОВНИХ СИГНАЛІВ

6.1 Мета роботи

1. Вивчити основні методи, параметри і характеристики, що визначають якість приховування мовних сигналів у каналах зв'язку.
2. Вивчити принципи дії і параметри пристроїв маскування мовного сигналу.
3. Вивчити методи виміру якості мовного сигналу.
4. Дослідити розбірливість слів у різних точках тракту перетворення мовного сигналу.
5. Дослідити спектри сигналів у різних точках тракту перетворення.
6. Розрахувати розбірливість слів для досліджуваної схеми маскування.

6.2 Загальні відомості

6.2.1 Скремблери

У системах зв'язку відомо два основні методи приховування мовних сигналів, що розрізняються за способом передавання по каналах зв'язку: аналогове скремблювання і дискретизація мови з подальшим шифруванням. Під **скремблюванням** розуміється зміна характеристик мовного сигналу таким чином, що одержаний модульований сигнал, володіючи властивостями нерозбірливості і невпізнання, займає ту ж смугу частот, що і початковий сигнал.

Кожний з цих методів має свої переваги і недоліки.

Так, для **аналогових скремблерів** характерна присутність під час передавання в каналі зв'язку фрагментів початкового відкритого мовного повідомлення, перетвореного в частотній і (або) часовій області. Це означає, що зловмисники можуть спробувати перехопити і проаналізувати передавану інформацію, на рівні звукових сигналів. Досвід свідчить, що новітні алгоритми аналогового скремблювання здатні забезпечити дуже високий рівень приховування.

Цифрові скремблери не передають якої-небудь частини початкового мовного сигналу. Мовні компоненти кодуються в цифровий

потік даних, який змішується з псевдовипадковою послідовністю, що виробляється ключовим генератором по одному з криптографічних алгоритмів. Підготовлене таким чином повідомлення передається за допомогою модему в канал зв'язку, на приймальному кінці якого проводяться зворотні перетворення з метою отримання відкритого мовного сигналу.

Технологія створення широкосмугових систем, призначених для приховування мови, добре відома, а її реалізація не уявляє особливих труднощів. При цьому використовуються такі методи кодування мови, як АДІКМ (адаптивна диференціальна імпульсно-кодова модуляція), ДМ (дельта-модуляція) і т.ін. Але представлена таким чином дискретизована мова може передаватися лише по спеціально виділеним широкосмуговим каналам зв'язку із смугою пропускання 4,8–19,2 кГц. Це означає, що вона не придатна для передачі по лініях телефонної мережі загального користування, де необхідна швидкість передавання даних повинна складати не менше 2400 бит/с. У таких випадках використовуються вузькосмугові системи, головною проблемою при реалізації яких є висока складність алгоритмів зняття мовних сигналів, здійснюваних у **вокодерних пристроях**.

За допомогою дискретного кодування мови з подальшим шифруванням завжди досягався високий ступінь приховування. Раніше цей метод мав обмежене застосування в наявних вузькосмугових каналах із-за низької якості відновлення передаваної мови. Досягнення в розвитку технологій низькошвидкісних дискретних кодерів дозволили значно поліпшити якість мови без зниження надійності приховування.

Аналогові скремблери підрозділяються на:

- мовні скремблери простих типів на базі часових і (або) частотних перестановок мовного сигналу (рис. 6.1);
- комбіновані мовні скремблери на основі частотно-часових перестановок відрізків мови, представлених дискретними відліками, із застосуванням цифрової обробки сигналів (рис. 6.2).

Цифрові системи приховування мови підрозділяються на широкосмугові (рис. 6.3) і вузькосмугові (рис. 6.4).

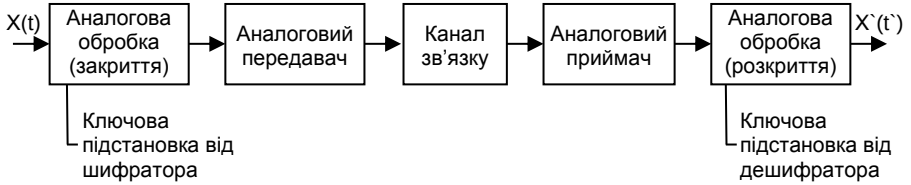


Рисунок 6.1- Схема простого мовного скремблера.

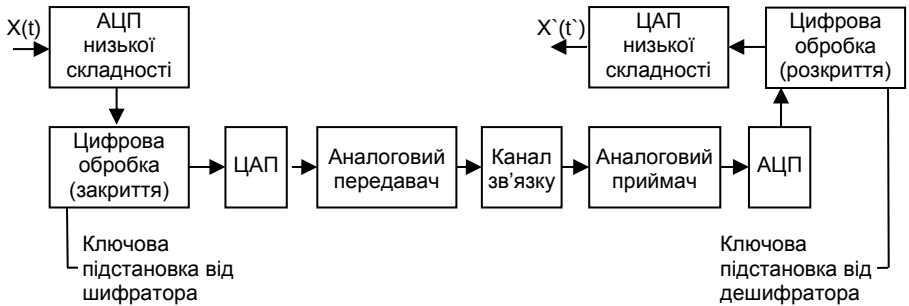


Рисунок 6.2- Схема комбінованого мовного скремблера.

Оцінюючи рівень захисту систем закриття мови, слід зазначити, що це поняття вельми умовне. При цьому слід констатувати, що у ряді виробів основні рівні захисту визначаються, як **тактичний** і **стратегічний**, що в деякому розумінні перекликається з поняттями практичної і теоретичної *стійкості криптосистем приховування даних*.

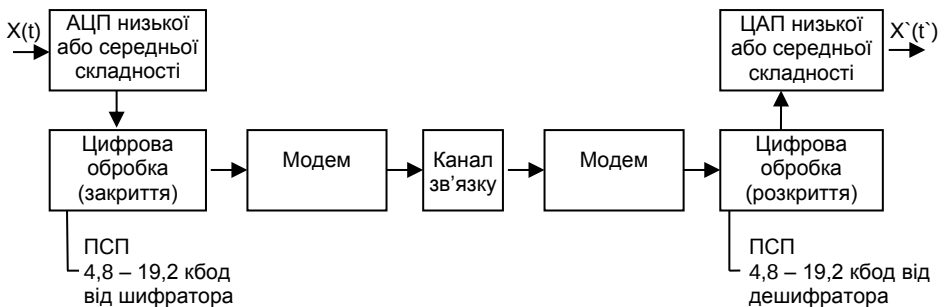


Рисунок 6.3. Схема широкопasmової системи приховування мови.

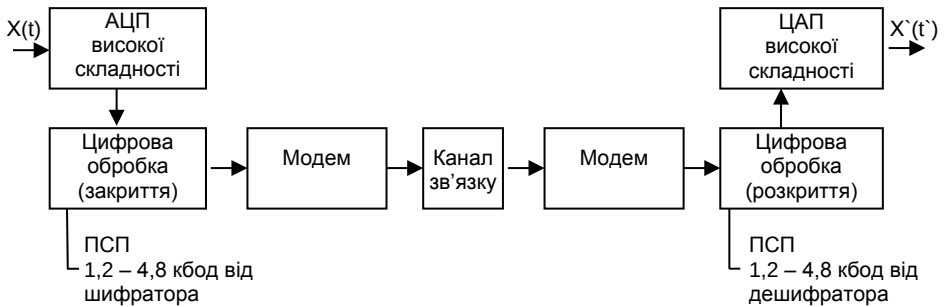


Рисунок 6.4. Схема вузькосмугової системи приховування мови.

Тактичний, або низький, рівень використовується для захисту інформації від прослуховування сторонніми особами на період, вимірюваний від хвилин до днів. Існує багато простих методів і способів забезпечення такого рівня захисту з прийнятною стійкістю.

Стратегічний, або високий, рівень захисту інформації від перехоплення використовується в ситуаціях, які мають на увазі, що висококваліфікованому, технічно добре оснащеному фахівцю буде потрібно для дешифрування перехопленого повідомлення період часу від декількох місяців до декількох років.

Слід зазначити, що таке поняття, як *якість відновленої мови*, є достатньо умовним, оскільки під ним звичайно розуміють факт пізнання абонента і розбірливість сигналу, що приймається.

6.2.2 Аналогове скремблювання

Серед сучасних пристроїв приховування мовних сигналів найбільше розповсюдження мають пристрої, що використовують метод аналогового скремблювання. Це дозволяє, по-перше, понизити вартість таких пристроїв, по-друге, ця апаратура застосовується в більшості випадків в стандартних телефонних каналах із смугою 3 кГц, по-третє, вона забезпечує комерційну якість дешифрованої мови, і, по-четверте, гарантує достатньо високий ступінь приховування.

Аналогові скремблери перетворюють початковий мовний сигнал за допомогою зміни його амплітудних, частотних і часових параметрів в різних комбінаціях. Скрембльований сигнал потім може бути переданий

по каналу зв'язку в тій же смузі частот, що і відкритий. У апаратах такого типу використовується один або декілька наступних **принципів аналогового скремблювання**.

Скремблювання в частотній області: частотна інверсія (перетворення спектру сигналу за допомогою гетеродину і фільтру), частотна інверсія із зсув (частотна інверсія із змінним стрибкоподібним зсувом несівної частоти), розділення смуги частот мовного сигналу на ряд піддіапазонів з подальшою їх перестановкою і інверсією.

Скремблювання в часовій області — розбиття фрагментів на сегменти з перемішуванням їх за часом з подальшим прямим і (або) інверсним прочитуванням.

Комбінація часового і частотного скремблювання.

Як правило, всі перестановки яким-небудь чином виділених сегментів або ділянок мови в часовій і (або) в частотній областях здійснюються за законом псевдовипадкової послідовності (ПВП). ПВП виробляється шифратором з ключом, який змінюється від одного мовного повідомлення до іншого.

На стороні приймача виконується дешифрування цифрових кодів, одержаних з каналу зв'язку, і перетворення їх в аналогову форму. Системи, робота яких заснована на такому методі, є достатньо складними, оскільки для забезпечення високої якості передаваної мови потрібна висока частота дискретизації вхідного аналогового сигналу і, відповідно, висока швидкість передачі даних (не менше 2400 бод). За таким же принципом можна розділити і пристрої дискретизації мови з подальшим шифруванням.

Не зважаючи на всю свою складність, апаратура даного типу використовується в комерційних структурах, більшість з яких передає дані по каналу зв'язку зі швидкостями модуляції від 2,4 до 19,2 кбит/с, забезпечуючи при цьому дещо гіршу якість відтворення мови в порівнянні із звичайним телефоном. Основною ж перевагою таких цифрових систем кодування і шифрування залишається високий ступінь закриття мови. Це досягається за допомогою використання широкого набору криптографічних методів, вживаних для захисту передачі даних по каналах зв'язку.

Оскільки скрембльовані мовні сигнали в аналоговій формі лежать в тій же смузі частот, що і початкові сигнали, це означає, що їх можна передавати по звичайних каналах зв'язку, що використовуються для передачі мови, без якого-небудь спеціального устаткування (модему).

Тому пристрої мовного скремблювання не такі дорогі і значно простіші, ніж пристрої дискретизації з подальшим цифровим шифруванням.

За режимами роботи аналогові скремблери можна розбити на два класи:

статичні системи, схема кодування яких залишається незмінною протягом всієї передачі мовного повідомлення;

динамічні системи, що постійно генерують кодові підстановки в ході передачі (код може бути змінений в процесі передачі протягом кожної секунди).

Очевидно, що динамічні системи забезпечують вищий ступінь захисту, оскільки різко обмежують можливість легкого прослуховування переговорів сторонніми особами.

Процес аналогового скремблювання є складним перетворенням мовного сигналу з його подальшим відновленням після проходження перетвореного сигналу по вузькосмуговому каналу зв'язку, в умовах дії шумів і завад. Можливе *перетворення мовного сигналу за трьома параметрами: амплітуді, частоті і часу*. Вважається, що використовувати амплітуду недоцільно, оскільки співвідношення сигнал/шум, що змінюється в часі, роблять надзвичайно складним завдання точного відновлення амплітуди сигналу. Тому практичне застосування одержали тільки частотне і часове скремблювання, а також їх комбінації.

Існує два основні види **частотних скремблерів** — **інверсні і смугові**. Обидва засновані на перетвореннях спектру початкового мовного сигналу для приховування передаваної інформації і відновлення одержаного повідомлення шляхом зворотніх перетворень.

Інверсний скремблер (рис. 6.5) здійснює перетворення мовного спектру, рівносильне повороту частотної смуги мовного сигналу навколо деякої частоти. При цьому досягається ефект перетворення низьких частот у високі і навпаки.

Даний спосіб забезпечує невисокий рівень приховування, оскільки у разі перехоплення легко встановлюється значення частоти, відповідне середній точці інверсії в смузі спектру мовного сигналу.

Деяке підвищення рівню приховування забезпечує **смугово-зсувний інвертор**, що розділяє смугу на дві субсмуги. При цьому точка розбиття виступає в ролі деякого ключа системи.

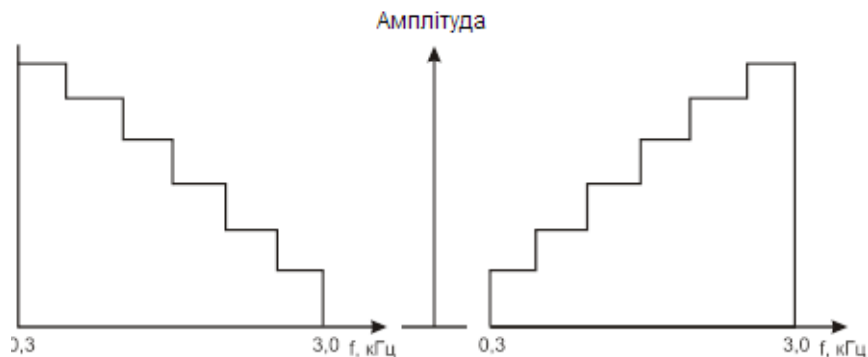


Рисунок 6.5- Принцип роботи інвертора мови.

Надалі кожна субсмуга може інвертуватися навколо своєї середньої частоти. Цей вид скремблювання, проте, також дуже простий для розкриття при перехопленні і не забезпечує надійного закриття. Підвищити рівень закриття можна шляхом зміни за деяким законом частоти, відповідній точці розбиття на смуги мовного сигналу (**ключа системи**).

Мовний спектр можна також розділити на декілька частотних смуг рівної ширини і провести їх перемішування і інверсію за деяким правилом (ключ системи). Так функціонує **смуговий скремблер** (рис. 6.6).

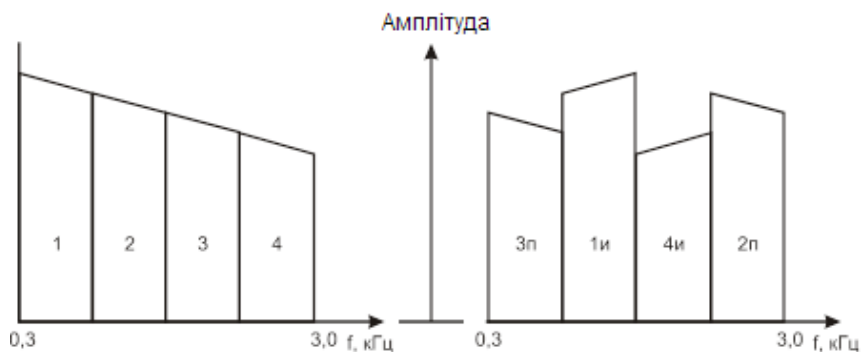


Рисунок 6.6 - Принцип роботи чотирьохсмугового скремблера.

Зміна ключа системи дозволяє підвищити ступінь закриття, але вимагає введення синхронізації на приймальній стороні системи. Основна частина енергії мовного сигналу зосереджена в невеликій області низькочастотного спектру, тому вибір варіантів перемішування обмежений, і багато систем характеризуються відносно високою залишковою розбірливістю.

Істотне підвищення ступеню закриття мови може бути досягнуте шляхом реалізації в смуговому скремблері *швидкого перетворення Фур'є* (ШПФ). При цьому кількість допустимих перемішувань частотних смуг значно збільшується, що забезпечує високий ступінь закриття без погіршення якості мови. Можна додатково підвищити ступінь закриття шляхом здійснення затримок різних частотних компонент сигналу на різну величину. Схему такої системи показано на рис. 6.7.

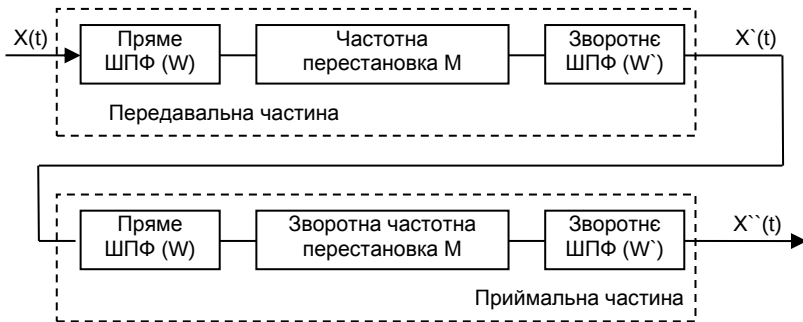


Рисунок 6.7 - Основна форма реалізації аналогового скремблера на основі ШПФ.

Головним недоліком використання ШПФ є виникнення в системі великої затримки сигналу (до 300 мс), обумовленою необхідністю використання вагових функцій. Це призводить до утруднень в роботі дуплексних систем зв'язку.

Часові скремблери засновані на двох основних способах приховування: *інверсії за часом сегментів мови* і їх *часовій перестановці*. В порівнянні з частотними скремблерами, затримка у часових скремблерів набагато більше, але існують різні методи її зменшення.

У скремблерах з **часовою інверсією** мовний сигнал ділиться на послідовність часових сегментів, кожний з яких передається інверсно в

часі — з кінця. Такі скремблери забезпечують обмежений рівень закриття, залежний від тривалості сегментів. Для досягнення нерозбірливості повільної мови необхідно, щоб довжина сегментів складала близько 250 мс. Затримка системи у такому разі складає близько 500 мс, що може виявитися неприйнятним в деяких додатках.

Для підвищення рівня приховування вдаються до способу перестановки часових відрізків мовного сигналу в межах фіксованого кадру (рис. 6.8).

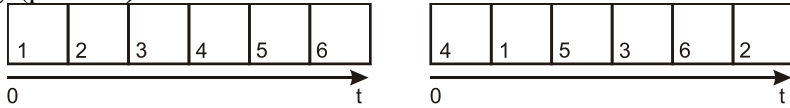


Рисунок 6.8 -. Схема роботи часового скремблера з перестановками у фіксованому кадру.

Правило перестановок є *ключем системи*, зміною якого можна істотно підвищити ступінь приховування мови. Залишкова розбірливість залежить від довжини відрізків сигналу і довжини кадру (чим довше останній, тим гірше розбірливість). Головний недолік скремблера з фіксованим кадром — великий інтервал часу затримки (приблизно 2 кадри). Цей недолік усувається в скремблері з перестановкою тимчасових відрізків мовного сигналу з *ковзаючим вікном*. У ньому кількість перестановок обмежена так, щоб затримка не перевищувала встановленого максимального значення. Кожний відрізок початкового мовного сигналу має так би мовити тимчасове вікно, усередині якого він може займати довільне місце при скремблюванні. Це вікно ковзає в часі у міру надходження в нього кожного нового відрізка сигналу. Затримка при цьому знижується до тривалості вікна.

Використовуючи комбінацію тимчасового і частотного скремблювання, можна значно підвищити ступінь приховування мови. **Комбінований скремблер** набагато складніше за звичайний і вимагає компромісного вирішення з вибору рівня приховування, залишкової розбірливості, часу затримки, складності системи і ступеню спотворень у відновленому сигналі. Кількість же всіляких систем, що працюють за таким принципом, обмежена лише уявою розробників.

Як приклад такої системи, розглянемо скремблер, схема якого представлена на рис. 6.9. У цьому скремблері операція частотно-часових перестановок дискретизованих відрізків мовного сигналу здійснюється за допомогою чотирьох процесорів цифрової обробки сигналів, один з

яких може реалізовувати функцію генератора псевдовипадкової послідовності.

У такому скремблері спектр оцифрованого аналого-цифровим перетворенням мовного сигналу розбивається за допомогою використання алгоритму цифрової обробки сигналу на частотно-часові елементи. Ці елементи потім перемішуються на частотно-часовій площині відповідно до одного з криптографічних алгоритмів (рис. 6.10) і підсумовуються, не виходячи за межі частотного діапазону початкового сигналу.

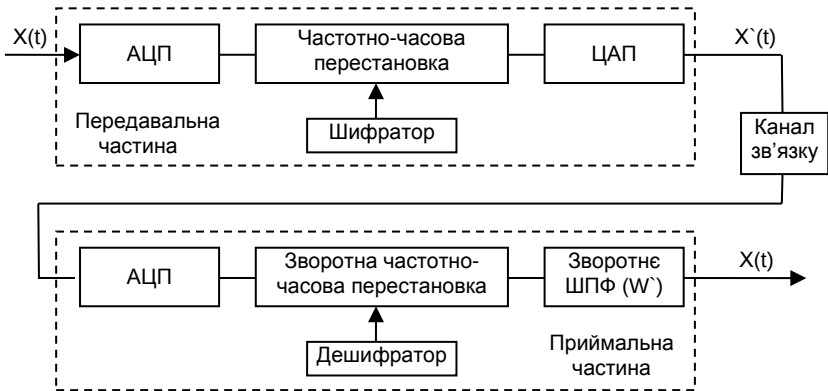


Рисунок 6.9 - Блок-схема комбінованого скремблера.

У представленій на рис. 6.10 системі приховування мови використовується чотири процесори цифрової обробки сигналів. Кількість частотних смуг спектру, в яких проводяться перестановки з можливою інверсією спектру, дорівнює чотирьом. Максимальна затримка частотно-часового елементу за часом дорівнює п'яти дискретизованим відлікам мовного сигналу. Одержаний таким чином приховуваний сигнал за допомогою ЦАП переводиться в аналогову форму і подається до каналу зв'язку.

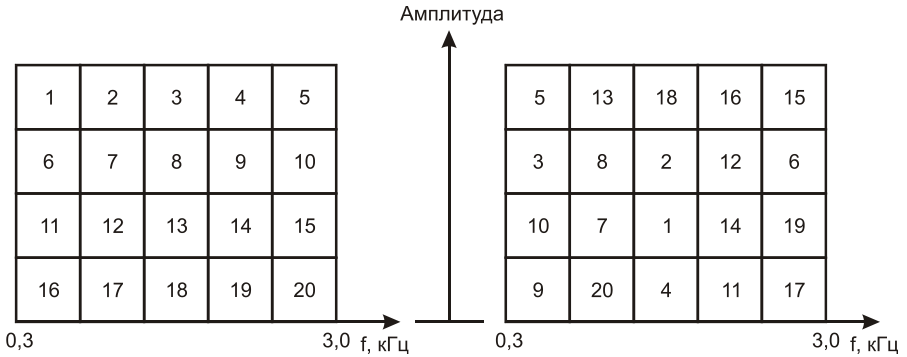


Рисунок 6.10 - Принцип роботи комбінованого скремблера.

На приймальному кінці проводяться зворотні операції з відновлення одержаного приховуваного мовного повідомлення. Стійкість представленого алгоритму порівняна із стійкістю систем цифрового закриття мови.

Скремблери всіх типів, за винятком простого (з частотною інверсією), вносять спотворення у відновлений мовний сигнал. Межі часових сегментів порушують цілісність сигналу, що неминуче призводить до появи позасмугових частотних складових. Небажаний вплив роблять і групові затримки складових мовного сигналу в каналі зв'язку. Результатом спотворень є збільшення мінімально допустимого співвідношення сигнал/шум, при якому може здійснюватися надійний зв'язок.

Проте, не дивлячись на вказані проблеми, методи часового і частотного скремблювання, а також комбіновані методи успішно використовуються в комерційних каналах зв'язку для захисту конфіденційної інформації.

6.2.3 Цифрове скремблювання

Альтернативним аналоговому скремблюванню мови є шифрування мовних сигналів, перетворених в цифрову форму, перед їх передачею (див. рис.6.3). Цей метод забезпечує вищий рівень приховування в порівнянні з описаними вище аналоговими методами. В основі пристроїв, що працюють за таким принципом, лежить представлення мовного сигналу у вигляді цифрової послідовності, що приховується за

одним з криптографічних алгоритмів. Передавання даних, що представляють дискретизовані відліки мовного сигналу або його параметрів, телефонними мережами, як і у разі пристроїв шифрування алфавітно-цифрової і графічної інформації, здійснюється через пристрої, звані *модемами*.

Основною метою під час розробки пристроїв цифрового приховування мови є збереження тих її характеристик, які найбільш важливі для сприйняття слухачем. Одним з шляхів є *збереження форми мовного сигналу*. Цей напрям застосовується в широкосмугових цифрових системах приховування мови. Проте ефективніше використовувати *властивості надлишковості цієї інформації*, що міститься в мові людини. Цей напрям розробляється у *вузькосмугових цифрових системах приховування мови*.

Ширину спектру мовного сигналу можна вважати приблизно рівною 3,3 кГц, а для досягнення хорошої якості сприйняття необхідне співвідношення сигнал/шум приблизно 30 дБ. Тоді, згідно теорії Шеннона, необхідна швидкість передачі дискретизованої мови відповідатиме величині 33 кбіт/с.

З іншого боку, мовний сигнал є послідовністю фонем, що передають інформацію. У англійській мові, наприклад, близько 40 фонем, в німецькій — близько 70 і т.д. Таким чином, для представлення фонетичного алфавіту потрібно приблизно 6-7 біт. Максимальна швидкість вимови не перевищує 10 фонем в секунду. Отже, мінімальна швидкість передачі основної технічної інформації мови — не менше 60-70 біт/с.

Збереження форми сигналу вимагає високої швидкості передачі і, відповідно, використання широкосмугових каналів зв'язку. Так при імпульсно-кодovій модуляції (ІКМ), використовуваний в більшості телефонних мереж, необхідна швидкість передачі, рівна 64 кбіт/с. У разі застосування адаптивної диференціальної ІКМ швидкість знижується до 32 кбіт/с і нижче. Для вузькосмугових каналів, які не забезпечують такі швидкості передавання, потрібні пристрої, що зменшують надлишковість мови до її передачі. Зниження інформаційної надлишковості мови досягається параметризацією мовного сигналу, при якій зберігаються істотні для сприйняття характеристики мови.

Таким чином, правильне застосування методів цифрової передачі мови з високою інформаційною ефективністю, є вкрай важливим напрямом розробки пристроїв цифрового приховування мовних сигналів.

У таких системах пристрій кодування мови (**вокодер**), аналізуючи форму мовного сигналу, проводить оцінку параметрів змінних компонент моделі генерації мови і передає ці параметри в цифровій формі по каналу зв'язку на синтезатор, де згідно цієї моделі по прийнятих параметрах синтезується мовне повідомлення. На малих інтервалах часу (до 30мс) параметри сигналу можуть розглядатися, як постійні. Чим коротший інтервал аналізу, тим точніше можна представити динаміку мови, але при цьому повинна бути вищою швидкість передавання даних. В більшості випадків на практиці використовуються інтервали 20-мілісекунд, а швидкість передачі досягає 2400 біт/с.

*Найбільш поширеними типами вокодерів є **смугові і з лінійним прогнозом**. Метою будь-якого вокодера є передача параметрів, що характеризують мову і що мають низьку інформаційну швидкість. **Смуговий вокодер досягає цієї мети шляхом передачі амплітуди декількох частотних смуг мовного спектру**.* Кожний смуговий фільтр такого вокодера збуджується при попаданні енергії мовного сигналу в його смугу пропускання. Оскільки спектр мовного сигналу змінюється відносно поволі, набір амплітуд вихідних сигналів фільтрів утворює придатну для вокодера основу. У синтезаторі параметри амплітуди кожного каналу керують коефіцієнтами підсилення фільтру, характеристики якого подібні характеристикам фільтру аналізатора. Таким чином, структура смугового вокодера базується на двох блоках фільтрів — для аналізу і для синтезу. Збільшення кількості каналів покращує розбірливість, але при цьому потрібна велика швидкість передачі. Компромісним рішенням звичайно стає вибір 16-20 каналів при швидкості передавання даних близько 2400 біт/с.

Смугові фільтри в цифровому виконанні будуються на базі аналогових фільтрів Баттерворта, Чебишева, еліптичних і ін. Кожний відрізок 20-мілісекунд часу кодується 48 бітами, з них 6 біт відводиться на інформацію про основний тон, один біт на інформацію “тон–шум”, що характеризує наявність або відсутність вокалізованої ділянки мовного сигналу, інші 41 біт описують значення амплітуд сигналів на виході смугових фільтрів.

Існують різні модифікації смугового вокодера, пристосовані для каналів з обмеженою смугою пропускання. За відсутності жорстких вимог на якість синтезованої мови вдається понизити кількість біт передаваної інформації з 48 до 36 на кожні 20 мс, що забезпечує зниження швидкості до 1200 біт/с. Це можливо у разі передачі кожного

другого кадру мовного сигналу і додаткової інформації про синтез пропущеного кадру. Втрати від процедур синтезу мови не є дуже великими, перевагою ж є зниження швидкості передачі сигналів.

Найбільшого поширення серед систем цифрового кодування мови з подальшим шифруванням набули системи, основним вузлом яких є **вокодери з лінійним прогнозом мови (ЛПМ)**.

Математичне представлення моделі цифрового фільтру, використовуваного у вокодері з лінійним прогнозом, має вигляд шматково-лінійної апроксимації процесу формування мови з деякими спрощеннями: кожний поточний відлік мовного сигналу є лінійною функцією **P** попередніх відліків. Не дивлячись на недосконалість такої моделі, її параметри забезпечують прийнятне представлення мовного сигналу. У вокодера з лінійним уявленням аналізатор здійснює мінімізацію помилки прогнозу, що є різницею поточного відліку мовного сигналу і середньозваженої суми попередніх відліків. Існує декілька методів мінімізації помилки. Загальним для всіх є те, що при оптимальній величині коефіцієнтів прогнозу спектр сигналу помилки наближається до білого шуму і сусідні значення помилки мають мінімальну корекцію. Відомі методи діляться на дві категорії: **послідовні** і **блокові**, які набули найбільшого поширення.

У вокодера з **лінійним прогнозом** мовна інформація передається трьома параметрами: амплітудою, співвідношенням “тон/шум” і періодом основного струму для вокалізованих звуків. Так, згідно федерального стандарту США, період аналізованого відрізка мовного сигналу складає 22,5 мс, що відповідає 180 відлікам при частоті дискретизації 8 кГц. Кодування в цьому випадку здійснюється 54 бітами, що відповідає швидкості передачі 2400 бит/с. При цьому 41 біт відводиться на кодування десяти коефіцієнтів прогнозу, 5 — на кодування величини амплітуди, 7 — на передачу періоду основного тону і 1 біт визначає рішення “тон/шум”. При здійсненні подібного кодування вважається, що всі параметри незалежні, проте в природній мові параметри корельовані і можливе значне зниження мінімально допустимої швидкості передачі даних без втрати якості, якщо правило кодування оптимізувати з урахуванням залежності всіх параметрів. Такий підхід відомий під назвою *векторного кодування*. Його застосування до вокодера з лінійним прогнозом дозволяє понизити швидкість передачі даних 800 бит/с і менш, з дуже малою втратою якості.

Основною особливістю використання систем цифрового приховування мовних сигналів є необхідність використання модемів. Можливі наступні підходи до проектування систем приховування мовних сигналів.

1.Цифрова послідовність параметрів мови з виходу вокодерного пристрою подається на вхід шифратора, де піддається перетворенню по одному з криптографічних алгоритмів, потім поступає через модем в канал зв'язку, на приймальній стороні якого здійснюються зворотні операції по відновленню мовного сигналу, в яких задіяні модем і дешифратор (див. рис. 6.3, 6.4). Модем є окремим пристроєм, що забезпечує передачу даних по одному з протоколів, рекомендованих МККТТ. Шифруючі/дешифруючі функції забезпечуються або в окремих пристроях, або в програмно-апаратній реалізації вокодеру.

2.Шифруючі/дешифруючі функції забезпечуються самим модемом (так званий модем, що засекречує), звичайно по відомих криптографічних алгоритмах типу DES і т.п. Цифровий потік, що несе інформацію про параметри мови, з виходу вокодеру поступає безпосередньо в такий модем. Організація зв'язку по каналу аналогічна приведеній вище.

6.2.4 Критерії оцінки систем приховування мови

Існує чотири основні критерії, за якими оцінюються характеристики пристроїв приховування мовних сигналів, а саме: ***розбірливість мови; впізнаність того, хто говорить; ступінь приховування і основні технічні характеристики системи.***

Прийнятною комерційною якістю відновленої на прийальному кінці мови вважається така, коли слухач може без вагань визначити голос того, хто говорить і сенс вимовленого повідомлення. Крім цього, під хорошою якістю передаваного мовного сигналу мається на увазі і можливість відтворення емоційних відтінків і інших специфічних ефектів розмови.

При використанні радіоканалів труднощі з розбірливості і впізнаності ще більш зростають із-за невизначеності умов поширення радіохвиль, і досягти повторюваності результатів неможливо без застосування моделей радіоканалів. Для дуплексних систем додатковий вплив на якість робить часова затримка сигналу, що вноситься мовним

скремблером або шифратором. Оскільки основним показником секретності передаваних мовних повідомлень є його нерозбірливість у разі перехоплення зломисником, порівняння по ступенях захисту є визначальним моментом при виборі користувачем конкретної системи закриття мови.

Як правило, аналогові скремблери використовуються там, де застосування цифрових систем приховування мови утруднене з-за наявності можливих помилок передавання (наземні лінії зв'язку з поганими характеристиками або канали дальнього радіозв'язку), забезпечують тактичний рівень захисту і добре оберігають переговори від сторонніх “випадкових вух”, що мають обмежені ресурси, будь то сусіди або товариші по службі. Для таких застосувань годяться системи із статичним закриттям, тобто що здійснюють шифрування за допомогою фіксованого ключа.

Якщо ж необхідно зберегти конфіденційність інформації від можливих конкурентів, що володіють достатнім технічним і спеціальним оснащенням, то потрібно застосовувати аналогові скремблери середнього рівня закриття з динамічно змінним в процесі розмови ключем. Природньо, що ці системи будуть дорожчі, ніж системи приховування з фіксованим ключем, проте вони настільки ускладнюють роботу зломисників по розробці дешифруючого алгоритму, що час, витрачений на це, значно знецінить здобуту інформацію з перехопленого повідомлення.

Оскільки у вітчизняних пристроях приховування, як правило, перед початком повідомлення передається синхропослідовність, в якій міститься частина додаткової інформації про ключ поточного передаваного повідомлення, у зломисника є тільки один шанс спробувати його розкрити, перебравши безліч ключових установок. Якщо ключі міняються щодня, то навіть у разі відомого алгоритму перетворення мови зломиснику доведеться перебрати багато тисяч варіантів у пошуках дійсної ключової послідовності.

Слід зазначити, що в системах засекречування мови, заснованої на шифрі перестановки N мовних елементів, загальна кількість ключів-перестановок дорівнює $N!$. Проте це значення не відображає реальної криптографічної стійкості системи із-за надлишковості інформації, що міститься в мовному сигналі, а також з-за розбірливості недосконалим чином переставленої і інвертованої мови. Тому криптоаналітику часто необхідно випробувати лише $K \ll N!$ випадкових перестановок для

розкриття мовного коду. Цей момент слід враховувати під час вибору надійної системи аналогового скремблювання.

6.3 Завдання на підготовку до лабораторної роботи

1. Вивчити основні методи, параметри і характеристики, що визначають якість приховування мовних сигналів у каналах зв'язку.
2. Вивчити принципи дії і параметри пристроїв маскування мовного сигналу.
3. Вивчити методи виміру якості мовного сигналу.
4. Вивчіть функціональну схему робочого місця (рис.6.11) для дослідження маскувача мовних сигналів.
5. Вивчіть схему і передню панель (рис.6.12) маскувача мовних сигналів.
6. Вивчіть описи й інструкцію з експлуатації аналізатору спектра та порядок роботи на ньому.

6.4 Контрольні запитання для самоперевірки і контролю підготовленості студентів до роботи

1. Чим пояснюється практична необхідність застосування маскувачів мовного сигналу?
2. У чому переваги і недоліки маскувачів з інверсією спектру ?
3. Як діють маскувачі з інверсією спектр?
4. Які основні параметри і характеристики маскувачів з інверсією спектру?
5. До яких висновків приводить аналіз акустичного прослуховування мовного сигналу в різних точках схеми маскувача.
6. Що являє собою аналогове та цифрове скремблювання?
7. Які структурні схеми мають різні типи скремблерів?
8. Що являють собою смугові вокодери та вокодери з лінійним прогнозом?
9. Які існують критерії оцінки систем закриття мови?
10. Для чого застосовуються артикуляційні іспити на розбірливість слів?

6.5 Матеріали, інструмент, прилади, обладнання

Функціональна схема лабораторного пристрою і робочого місця для дослідження маскувача мовних сигналів наведена на рис. 6.11. Її основу складають джерело сигналу; маскувач; акустичний контроль; аналізатор спектру та програмне забезпечення.



Рисунок 6.11 - Функціональна схема робочого місця для дослідження маскувача мовних сигналів.

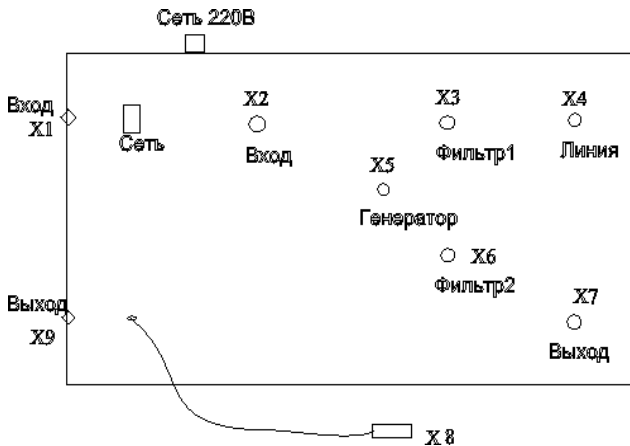


Рисунок 6.12- Вигляд передньої панелі маскувача мовних сигналів.

6.6 Вказівки з техніки безпеки

1. По ступеню захисту від поразки електричним струмом прилади відносяться до класу захисту 01 відповідно до вимог ДСТУ 4.275.003 – 77.

2. В приладах присутня висока напруга до 220 В, небезпечна для життя, тому при експлуатації, контрольно-профілактичних та регулювальних роботах, вироблюваних з приладом, необхідно строго дотримуватися відповідних запобіжних заходів, а також перед вмиканням приймачів перевірте наявність захисного заземлення:

– до включення мережевої вилки шнура живлення необхідно перевірити справність мережевого сполучного шнура та з'єднати клеми «» приладів з шиною захисного заземлення приміщення дротом перетином жили не меншого 4 мм;

– з'єднання клеми «» з шиною захисного заземлення, провести раніше інших пристосувань до приладів, а від'єднати – після всіх від'єднань;

– у випадках використання приладів сумісно з іншою апаратурою, при проведенні вимірювань, при обслуговуванні та ремонті з'єднати клеми «» всіх приладів з шиною захисного заземлення в цілях вирівнювання потенціалів їх корпусів;

– при ремонті приладів заміну будь-якого елемента проводити тільки при винятій з розетки мережевої вилки шнура живлення;

– при регулюванні та вимірюваннях в схемі приладу користуватися надійно ізольованим інструментом та пробниками.

– підключення і відключення від приладу кабелю допускається проводити тільки при вимкнених кнопках «СЕТЬ».

6.7 Порядок проведення лабораторної роботи

Експериментальна частина

1. Проведіть акустичний контроль мовних сигналів у різних точках схеми маскувача.

2. За допомогою таблиць, наведених у додатках проведіть артикуляційні іспити маскувача.

Обробка результатів досліджень

1. Порівняйте спектри сигналів у різних точках схеми маскувача.
2. Розгляньте склад неправильно прийнятих слів і , аналізуючи його, зробіть висновок про параметри перекручувань під час перетворення маскувачем.

6.8 Зміст звіту

1. Обґрунтуйте задачі і параметри маскування.
2. Наведіть основні алгоритми маскування мовних сигналів у каналах зв'язку.
3. Опишіть суб'єктивні відчуття акустичного прослуховування мовного сигналу в різних точках схеми.
4. Наведіть порівняльну таблицю слів, прийнятих після демаскування.

6.9 Рекомендована література

1. Бурячок В.Л. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. [Текст] / В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко. – К.: ДУТ, 2015. – 345 с.
2. Іванченко С.О. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник [Текст] / С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.
3. Вишня В.Б. Основи інформаційної безпеки: навч. посібник [Текст] / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. – 128 с.
4. Остапов С.Е. Технології захисту інформації: навчальний посібник [Текст] / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
5. Остапов С.Е. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. [Текст] / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020. – 678 с.

6.10 Додатки

Додаток 6.А

Таблиця 6.А.1 – Таблиця випадкових слів для проведення іспитів на розбірливість

Споживання	Пограничний	Опоясувати	Спідлоба
Взвод	Честь	Спаяний	Боець
Підкорювати	Паспортний	Людний	Стікатися
Креслити	Простота	Автомобіль	Рушати
Вимовити	Волога	Ланцюг	Фонд
Маневр	Чорний	Виводок	Напруга
Шлях	Залишитися	Можливість	Поганий
Карати	Парк	Всяляти	Квасоля
Бігом	Приголомшливий	Чиж	Виборець
Похмурий	Паровий	Додати	Недалеко
Експедиція	Прибуття	Землеробство	Мука
Вартувати	Вирішувати	Фирма	Момент
Лев	Зробити	Накульгувати	Переїзд
Литися	Натура	Критик	Відставити
Посягання	Відмінно	Зав'язувати	Всесвітній
Чути	Палата	Нісенітниця	Ромб
Остригати	Клас	Трьохшвидкісний	Зловживання
Рівнина	Кульгавий	Здатися	Конвеєр
Запис	П'ятниця	Омлет	Роздобути
Назовні	Підлеглий	Діяти	Слово
Дванадцятий	Крихкий	Змістовний	Вібрувати
Шпигун	Бігти	Поживний	Зібрати
Шепотітися	Молотьба	Витекти	Інтервал
Вигін	Нарис	Знайомство	Любити
Головувати	Зарядка	Дід	Бунтівний